Kaspersky Anti-Virus 6.0 para Windows Servers MP4

GUIA DO USUÁRIO

VERSÃO DO APLICATIVO: 6.0 PACOTE DE MANUTENÇÃO 4

Prezado usuário do Kaspersky Anti-Virus!

Obrigado por escolher nosso produto. Esperamos que esta documentação seja de ajuda no seu trabalho e forneça as respostas necessárias.

Este documento está sujeito a modificações sem prévio aviso. Para obter a última versão deste documento, visite o site da Kaspersky Lab em http://brazil.kaspersky.com/docs/.

Data da revisão: 09.07.2009

http://brazil.kaspersky.com/
http://brazil.kaspersky.com/suporte/

ÍNDICE

INTRODUÇÃO

NESTA SEÇÃO

CONTRATO DE LICENÇA DO USUÁRIO FINAL (EULA)

O Contrato de licença do usuário final é um contrato legal entre você e a Kaspersky Lab que especifica os termos dentro dos quais você pode usar o software que comprou.

Leia o EULA inteiro atentamente!

Se você não concordar com os termos do EULA, pode devolver seu produto na caixa ao revendedor onde o comprou e receberá como reembolso a quantidade que pagou pelo aplicativo, desde que o envelope que contém o disco de instalação esteja selado.

Ao abrir o envelope selado com o CD de instalação, você aceita todos os termos do EULA.

SERVIÇOS FORNECIDOS PARA USUÁRIOS REGISTRADOS

A Kaspersky Lab oferece um pacote amplo de serviços para todos os usuários registrados que lhes permite aumentar o desempenho do aplicativo.

Depois de comprar uma licença, você se torna um usuário registrado e, durante o período da sua licença, receberá os seguintes serviços:

- atualizações de hora em hora para os bancos de dados dos aplicativos e atualizações do pacote de software;
- suporte para temas relacionados com a instalação, a configuração e o uso do produto de software comprado. Os serviços serão fornecidos por telefone ou email;
- notificações sobre os novos produtos da Kaspersky Lab e os novos vírus que aparecem no mundo. Este serviço está disponível para os usuários que sejam assinantes do boletim de notícias da Kaspersky Lab no site de Serviço de suporte técnico (http://support.kaspersky.com/subscribe/).

Suporte para temas relacionados com o rendimento e o uso dos sistemas operativos, software de terceiros ou outras tecnologias, se não for fornecido.

REQUISITOS DO SISTEMA PARA HARDWARE E SOFTWARE

Para o funcionamento correto do Kaspersky Anti-Virus 6.0, o computador deve cumprir estes requisitos mínimos:

Requisitos gerais:

- 300 MB livres de espaço no disco rígido.
- Microsoft Internet Explorer 6.0, ou superior (para atualizar os bancos de dados do aplicativo e os módulos do programa por meio da Internet).

- Microsoft Windows Installer 2.0. ou superior.

Windows 2000 Server / Advanced Server (Service Pack 4 Rollup1), Windows Server 2003 Standard / Enterprise (Service Pack 2), Windows Server 2003 x64 Standard / Enterprise (Service Pack 2), Windows Small Business Server 2003:

- Processador Intel Pentium 400 MHz 32-bit (x86) / 64-bit (x64) ou superior (ou um equivalente compatível).
- 512 MB livres de RAM.

Windows Server 2003 R2 Standard / Enterprise Edition, Windows Server 2003 R2 x64 Standard / Enterprise Edition, Windows Server 2008 Standard / Enterprise (Service Pack 1 ou superior), Windows Server 2008 x64 Standard / Enterprise (Service Pack 1 ou superior), Windows Small Business Server 2008, Windows Essential Business Server 2008, Windows Server 2008 R2 x64 Standard / Enterprise:

- Processador Intel Pentium GHz 32 bits (x86) / 1.4 GHz 64 bits (x64) ou superior (ou um equivalente compatível).
- 1 GB livre de RAM.

KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS MP4

O Kaspersky Anti-Virus 6.0 para Windows Servers MP4 é uma nova geração de produtos para segurança de dados.

NESTA SEÇÃO

OBTENÇÃO DE INFORMAÇÕES SOBRE O APLICATIVO

Se tiver perguntas sobre a compra, a instalação ou o uso do Kaspersky Anti-Virus, as respostas serão disponíveis de imediato.

A Kaspersky Lab oferece várias fontes de informação sobre o aplicativo. Você pode escolher a opção mais apropriada, segundo a importância e a urgência da pergunta.

NESTA SEÇÃO

FONTES DE INFORMAÇÃO PARA PESQUISAR DE FORMA INDEPENDENTE

Você pode consultar as seguintes fontes de informação sobre o aplicativo:

- página do aplicativo no site da Kaspersky Lab;
- página do aplicativo no site do Serviço de suporte técnico (na Base de conhecimentos);
- sistema de ajuda;
- documentação.

Página do aplicativo no site da Kaspersky Lab

http://usa.kaspersky.com/support/corporate/server/

Esta página fornecerá informação geral sobre o aplicativo, seus características e opções.

Página do aplicativo no site do Serviço de suporte técnico (na Base de conhecimentos)

http://usa.kaspersky.com/support/corporate/server/windows/

Nesta página, você encontrará os artigos criados pelos especialistas do Serviço de suporte técnico.

Estes artigos contêm informação útil, recomendações e perguntas frequentes sobre compra, instalação e uso do aplicativo. Estão ordenados por tema, por exemplo, Administrar arquivos de chave, Configurar atualizações da base de dados ou Eliminar as falhas operacionais. Estes artigos podem responder as perguntas relacionadas não só com este aplicativo, mas também outros produtos da Kaspersky Lab. Também podem conter as notícias do Serviço de suporte técnico.

Sistema de ajuda

O pacote de instalação do aplicativo inclui o arquivo de ajuda completo e de contexto. Ele contém informações sobre como administrar a proteção do computador (visualizar estado de proteção, verificar várias áreas do computador para detectar vírus, executar outras tarefas) e a informação sobre cada janela do aplicativo, por exemplo, a lista das configurações apropriadas e sua descrição e a lista de tarefas por executar.

Para abrir o arquivo de ajuda, clique no botão **Ajuda** na janela desejada ou pressione a tecla **<F1>**.

Documentação.

O pacote de instalação do Kaspersky Anti-Virus inclui o documento do **Guia do usuário** (em formato .pdf). Este documento contém descrições das funções do aplicativo e das opções e os principais algoritmos operacionais.

CONTATO COM O DEPARTAMENTO DE VENDAS

Se tiver dúvidas sobre como escolher ou comprar o aplicativo ou ampliar sua licença, procure um de nossos distribuidores autorizados ou através dos telefones indicados no link a seguir: http://brazil.kaspersky.com/contacts/.

Você também pode enviar suas perguntas ao Departamento de Vendas através do preenchimento do formulário neste link: http://brazil.kaspersky.com/products/sales_info_request.php.

CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO

Se você já comprou o Kaspersky Anti-Virus, pode obter informações sobre o programa contatando o serviço de Suporte técnico, por telefone ou pela Internet.

Os especialistas do serviço de Suporte técnico responderão qualquer pergunta sobre como instalar e usar o aplicativo. Eles também ajudarão a eliminar as consequências das atividades de malware se seu computador tiver sido infectado.

Antes de se comunicar com o Serviço de Suporte técnico, leia os Termos e condições de suporte técnico (http://support.kaspersky.com/support/rules).

Solicitação por email ao Serviço de Suporte técnico

Você pode enviar sua pergunta aos especialistas do Serviço de Suporte técnico preenchendo o formulário online de atendimento remoto (http://brazil.kaspersky.com/suporte/).

Você pode perguntar em russo, inglês, alemão, francês ou espanhol.

Para enviar uma solicitação por email, você deve indicar a **identificação de cliente** obtida durante o registro no site do Serviço de Suporte técnico e sua **senha**.

Se você ainda não é um usuário registrado dos aplicativos da Kaspersky Lab, pode preencher um formulário de registrono endereço https://support.kaspersky.com/en/personalcabinet/registration/form/. Quando se registrar, deverá digitar o *código de ativação* ou o *nome do seu arquivo de chave da licença*.

O Serviço de Suporte técnico responderá sua solicitação na sua Conta Kaspersky (https://support.kaspersky.com/en/PersonalCabinet) e pelo email que você especificou na sua solicitação.

Descreva o problema que encontrou no formulário online da solicitação dando o maior detalhe possível. Especifique os seguintes dados nos campos obrigatórios:

- **Tipo de solicitação**. Selecione o tema que se corresponde mais especificamente com o problema, por exemplo: Problema com instalação/desinstalação do produto ou problema com a pesquisa/eliminação de vírus. Se você não encontrou um tema apropriado, selecione "Pergunta geral".
- **Nome de aplicativo e número de versão**.
- **Texto da solicitação**. Descreva o problema que encontrou dando o maior detalhe possível.
- **ID de cliente e senha**. Digite o número de cliente e a senha que recebeu durante o registro no site do serviço de Suporte Técnico.
- **Endereço de email**. O Serviço de Suporte técnico lhe enviará uma resposta para sua pergunta neste endereço de email.

Suporte técnico por telefone

Se tiver um problema urgente, pode ligar ao nosso Serviço de Suporte técnico local. Antes de se comunicar com os especialistas de Suporte técnico falantes de russo (http://support.kaspersky.ru/support/support_local) ou com os especialistas internacionais (http://support.kaspersky.com/support/international), reúna as informações (http://support.kaspersky.com/support/details) sobre seu computador e o aplicativo antivírus instalado nele. Isso permitirá que nossos especialistas possam ajudar mais rapidamente.

DISCUSSÃO DOS APLICATIVOS DA KASPERSKY LAB NO FÓRUM WEB

Se sua pergunta não exige uma resposta urgente, você pode falar com os especialistas da Kaspersky e com outros usuários em nosso fórum no endereço http://forum.kaspersky.com.

Nesse fórum, você pode ver os temas existentes, deixar seus comentários, criar novos temas e usar a ferramenta de pesquisa.

O QUE É NOVO NO KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS MP4

O Kaspersky Anti-Virus 6.0 é uma ferramenta integral de proteção de dados. Analisemos em detalhe as inovações no Kaspersky Anti-Virus 6.0.

Novidade em proteção:

- O novo antivírus kernel que usa o Kaspersky Anti-Virus detecta os programas prejudiciais mais eficazmente. Além disso, o novo antivírus kernel também é muito mais rápido para verificar o sistema e detectar vírus. É o resultado da melhora no processamento de objetos e do uso otimizado dos recursos do computador (particularmente para processadores duo ou quadro core).
- Um novo analisador heurístico tem sido implementado para fornecer uma detecção mais exata e bloquear os programas maliciosos previamente desconhecidos. Se a assinatura do programa não foi encontrada nos bancos de dados antivírus, o analisador heurístico simula o início do programa em um ambiente virtual isolado. Esse método é seguro e permite a análise de todos os efeitos de um programa antes de executá-lo em um ambiente real.
- O procedimento de atualização para o aplicativo foi aprimorado. O computador agora já quase não precisa ser reiniciado.

Novas características da interface:

- A interface simplifica as funções do programa e o torna fácil de usar.
- A interface foi redesenhada no que respeita às necessidades dos administradores de redes de tamanho pequeno a médio e dos administradores de grandes redes corporativas.

Novas funções no Kit de Administração Kaspersky:

- O Kit de Administração Kaspersky facilita e simplifica a administração dos sistemas de proteção antivírus de uma empresa. Os administradores podem usar o aplicativo para administrar a proteção de uma rede corporativa de qualquer tamanho, com milhares de nós, incluídos os usuários remotos e móveis.
- Uma função que permite a instalação remota do aplicativo com a última versão dos bancos de dados do aplicativo foi adicionada.
- O gerenciamento do aplicativo quando instalado em um computador remoto foi melhorado (a estrutura da política foi redesenhada).
- Uma característica foi adicionada e permite o uso da configuração de um aplicativo existente ao criar uma política.
- Outra característica importante é percebida na opção de criação de configurações específicas para usuários móveis ao configurar tarefas de atualização de grupo.
- Uma outra característica foi implementada e permite desativar temporalmente ações da política e tarefas de grupos para computadores clientes com o aplicativo instalado (após inserirem a senha correta).

EM QUE ESTÁ BASEADA A DEFESA DO KASPERSKY ANTI-VIRUS

A proteção do Kaspersky Anti-Virus para Windows Servers inclui:

- Antivírus de arquivos (ver página 13) que monitora o sistema de arquivos do computador em tempo real.
- Tarefas de verificação de vírus (ver página 14) que são usadas para verificar o computador inteiro ou pastas, arquivos, unidades e áreas separadas para detectar vírus.
- Atualizar (ver página 14) que garante o estado atualizado dos módulos do aplicativo interno e dos bancos de dados usados para detectar programas prejudiciais.
- Funções de apoio (veja seção "Funções de apoio do aplicativo" na página 14) que fornecem apoio de informações para trabalhar com o aplicativo e ampliar suas capacidades.

ANTIVÍRUS DE ARQUIVOS

O servidor está protegido em tempo real usando o Antivírus de arquivos.

Um sistema de arquivos pode conter vírus e outros programas perigosos. Os programas maliciosos podem ser armazenados no sistema de arquivos durante anos depois de um dia passarem para uma unidade removível ou da Internet sem se manifestarem nem um pouco. Mas basta abrir o arquivo infectado que o vírus será ativado instantaneamente.

Antivírus de arquivos é o componente que supervisa o sistema de arquivos do seu computador. Verifica todos os arquivos abertos, executados ou salvos no computador e todas as unidades de disco conectadas. O Kaspersky Anti-Virus intercepta todas as tentativas de acesso a um arquivo e verifica esse arquivo quanto à presença de vírus conhecidos. O arquivo poderá ser processado somente se não estiver infectado ou for neutralizado com êxito pelo

aplicativo. Se, por algum motivo, não for possível desinfetar um arquivo, ele será excluído e sua cópia será salva no Backup, ou ele será movido para a Quarentena.

TAREFAS DE VERIFICAÇÃO DE VÍRUS

Além da proteção do Antivírus de arquivos, é extremamente importante verificar os vírus do servidor ocasionalmente. Isso é necessário para descartar a possibilidade de disseminar programas prejudiciais que não foram descobertos pelo Antivírus de arquivos porque, por exemplo, o nível de segurança foi configurado como baixo, ou por outros motivos.

As seguintes tarefas de verificação de vírus estão incluídas no Kaspersky Anti-Virus:

Verificação

Verificação de objetos selecionados pelo usuário. Você pode verificar qualquer objeto do sistema de arquivos do computador.

Verificação completa

Uma verificação completa de todo o sistema. Os seguintes objetos são verificados por padrão: memória do sistema, programas carregados na inicialização, backup do sistema, bancos de dados de email, discos rígidos, mídias de armazenamento removíveis e unidades de rede.

Verificação rápida

Verificação de vírus nos objetos de inicialização do sistema operacional.

ATUALIZAÇÃO

Para bloquear qualquer ataque em rede, excluir um vírus ou outro programa prejudicial, o Kaspersky Anti-Virus deve ser atualizado regularmente. O componente **Atualização** foi desenhado para esse fim. Realiza a atualização das bases de dados e dos módulos usados pelo aplicativo.

O serviço de distribuição de atualização permite salvar as atualizações de bases de dados e os módulos programa baixados dos servidores da Kaspersky Lab em uma pasta local e depois conceder o acesso a partir de outros computadores da rede para evitar o tráfego da rede.

FUNÇÕES DE SUPORTE DO APLICATIVO

O Kaspersky Anti-Virus inclui uma série de funções de suporte. Elas foram desenhadas para manter atualizado o aplicativo, ampliar suas capacidades e ajudar você a usar o aplicativo.

Arquivos de dados

Quando o aplicativo é usado, cada componente de proteção, tarefa de verificação de vírus e atualização do aplicativo cria um relatório. Ele contém informações sobre as atividades realizadas e os resultados. Com isso, você pode conhecer os detalhes de como funciona o componente Kaspersky Anti-Virus. Se houver problemas, você pode enviar os relatórios à Kaspersky Lab para que nossos especialistas possam estudar a situação com mais detalhe e ajudar o antes possível.

O Kaspersky Anti-Virus move todos os arquivos suspeitos de serem perigosos para uma área especial de armazenamento chamada *Quarentena*. Esses arquivos são armazenados em forma criptografada para não infectar o computador. Você pode verificar se estes objetos contêm vírus, restaurá-los ao seu local anterior, excluí-los ou colocar os arquivos em quarentena. Todos os arquivos que não estão infetados depois de completar a verificação de vírus são restaurados automaticamente a seus locais anteriores.

O *Backup* mantém cópias dos arquivos desinfetados e excluídos pelo Kaspersky Anti-Virus. As cópias são criadas para que possa restaurar os arquivos ou obter uma imagem da infecção, se for necessário. As cópias de segurança dos arquivos também são armazenadas em forma criptografada para evitar mais infecções.

Você pode restaurar um arquivo da cópia de segurança ao local original e excluir a cópia.

Disco de recuperação

O Disco de recuperação é criado para verificar e desinfetar computadores infectados compatíveis com x86. Deve ser usado quando o nível de infecção está em um nível que não permite desinfetar o computador usando aplicativos antivírus ou utilitários de remoção.

Licença

Quando você compra o Kaspersky Anti-Virus, você passa a ter um contrato de licença com a Kaspersky Lab que rege o uso do aplicativo e seu acesso às atualizações de bancos de dados dos aplicativos e o Suporte técnico durante um período especificado. O prazo de uso e outras informações necessárias para a funcionalidade total do aplicativo são fornecidos na licença.

Usando a função **Licença**, você pode obter informações detalhadas sobre sua licença atual, a compra de uma nova licença ou a renovação da licença existente.

Suporte

Todos os usuários do Kaspersky Anti-Virus podem utilizar nosso Serviço de suporte técnico. Para ver as informações sobre onde obter o suporte técnico, use a função **Suporte**.

Usando os links fornecidos, você pode ir ao fórum de usuários dos produtos da Kaspersky Lab e procurar em uma lista de perguntas frequentes que podem oferecer uma solução para seu problema. Além disso, você pode preencher o formulário especial no site e enviar ao Suporte Técnico uma mensagem sobre um erro ou um comentário sobre a operação do programa.

Você também tem acesso ao Serviço de Suporte técnico online e, obviamente, nossos funcionários estão sempre prontos para oferecer-lhe suporte telefônico sobre o Kaspersky Anti-Virus.

INSTALAÇÃO DO KASPERSKY ANTI-VIRUS 6.0

O Kaspersky Anti-Virus 6.0 para Windows Servers MP4 pode ser instalado em um computador de várias formas:

- Instalação local – instalação do aplicativo em um único computador. Acesso direto a esse computador é necessário para executar e completar a instalação. A instalação local pode ser feita de um dos seguintes modos:
  - modo interativo, usando o assistente de instalação do aplicativo (veja seção "Instalação usando o assistente de instalação" na página 16). Este modo exige a participação do usuário na instalação;
  - modo não interativo no qual a instalação do aplicativo é executada desde a linha de comando e não requer a participação do usuário para instalar (veja seção "Instalação do aplicativo desde a linha de comando" na página 19).
- Instalação remota: instalação do aplicativo nos computadores em rede gerenciados em forma remota desde a estação de trabalho de um administrador usando o seguinte:
  - grupo de software do Kit de Administração Kaspersky (ver Guia de implantação do Kit de Administração Kaspersky);
  - políticas de domínio de grupo do Microsoft Windows Server 2000/2003 (veja seção "Instalação do editor do Objeto de política de grupo" na página 20).

Antes de começar a instalação do Kaspersky Anti-Virus (incluída a remota), é recomendável fechar todos os aplicativos ativos.

NESTA SEÇÃO

INSTALAÇÃO USANDO O ASSISTENTE DE INSTALAÇÃO

Para instalar o Kaspersky Anti-Virus no seu computador, execute o arquivo de instalação no CD do produto.

A instalação do aplicativo desde o arquivo de instalação descarregado pela Internet é idêntica à instalação do aplicativo desde o CD.

O programa de configuração é implementado como assistente padrão do Windows. Cada janela contém um grupo de botões para controlar o processo de instalação. Abaixo se encontra uma breve descrição do seu objetivo:

- **Avançar** – aceitar a ação e passar à etapa seguinte no procedimento de instalação.
- **Voltar** – voltar à etapa anterior no procedimento de instalação.
- **Cancelar** – cancelar a instalação.

- **Concluir** – completar o procedimento de instalação do aplicativo.

Abaixo se encontra uma discussão detalhada de cada etapa do pacote de instalação.

ETAPA 1. VERIFICAR SE O SISTEMA CUMPRE COM OS REQUISITOS DE INSTALAÇÃO

Antes de instalar o Kaspersky Anti-Virus no computador, o assistente verificará se o computador cumpre com os requisitos mínimos. Também verificará se você tem os direitos exigidos para instalar o software.

Se alguma das condições não for atendida, aparecerá a notificação correspondente na tela. É recomendável instalar as atualizações requeridas usando o serviço **Atualização de Windows** e os programas necessários antes de tentar reinstalar o Kaspersky Anti-Virus.

ETAPA 2. JANELA DE INÍCIO DA INSTALAÇÃO

Se seu sistema cumpre completamente as condições implícitas, imediatamente após o arquivo de instalação ser executado, a janela de início se abrirá na tela e mostrará a informação sobre o início da instalação do Kaspersky Anti-Virus.

Para proceder com a instalação, clique no botão **Avançar.** Para cancelar a instalação, pressione o botão **Cancelar**.

ETAPA 3. VISUALIZAÇÃO DO CONTRATO DE LICENÇA

A seguinte caixa de diálogo do aplicativo inclui o contrato de licença entre você e a Kaspersky Lab. Leia o contrato atentamente e se concordar com todos os termos e as condições, selecione a opção **Aceito os termos do Contrato de licença** e clique no botão **Avançar**. A instalação continuará.

Para cancelar a instalação, pressione o botão **Cancelar**.

ETAPA 4. SELEÇÃO DA PASTA DE INSTALAÇÃO

A etapa seguinte da instalação do Kaspersky Anti-Virus define a pasta para instalar o aplicativo. O caminho padrão é o seguinte:

- **<Drive>** → **Program Files** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** – para sistemas de 32 bits.

- **<Drive>** → **Program Files (x86)** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** – para sistemas de 64 bits.

Você pode especificar uma pasta diferente clicando no botão **Procurar** e selecionar uma pasta na janela de seleção de pasta padrão ou digitando o caminho da pasta no campo de entrada fornecido.

Leve em conta que se você digitar manualmente o caminho completo para a pasta de instalação, a extensão não deve superar os 200 caracteres e o caminho não deve conter caracteres especiais.

Para proceder com a instalação, clique no botão **Avançar.**

ETAPA 5. USO DAS CONFIGURAÇÕES DO APLICATIVO SALVAS APÓS A INSTALAÇÃO ANTERIOR

Nesta etapa, você pode especificar se deseja usar configurações de proteção e bancos de dados do aplicativo na operação do aplicativo se esses objetos foram salvos no seu computador depois que a versão anterior do Kaspersky Anti-Virus 6.0 foi removida.

Analisemos como ativar as funções descritas acima.

Se uma versão anterior (build) do Kaspersky Anti-Virus tinha sido instalada no seu computador e se você salvou os bancos de dados do aplicativo depois de ser removido, então pode integrá-los à versão que está instalando. Para fazê-lo, marque a caixa ☑ **Bancos de dados do aplicativo**. Os bancos de dados incluídos no pacote de instalação não serão copiados no servidor.

Para usar as configurações de proteção que você modificou em uma versão anterior em salvou em seu computador, verifique a caixa ☑ **Configurações de Aplicativos**.

ETAPA 6. SELEÇÃO DO TIPO DE INSTALAÇÃO

Nesta etapa, você deve definir o grau de completude da instalação do aplicativo. Há duas opções de instalação:

Completa. Neste caso, todos os componentes do Kaspersky Anti-Virus serão instalados no seu servidor. Para conhecer as etapas adicionais da instalação, consulte a Etapa 8.

Personalizado. Neste caso, você terá a opção de escolher qual dos componentes do aplicativo você deseja instalar. Para conhecer mais detalhes, consulte a Etapa 7.

Para selecionar o modo de instalação, pressione o botão correspondente.

ETAPA 7. SELEÇÃO DOS COMPONENTES DO APLICATIVO PARA A INSTALAÇÃO

Esta etapa será executada somente se você selecionou a opção de instalação **Personalizado**.

Antes de começar a instalação personalizada, deve escolher qual dos componentes do Kaspersky Anti-Virus deseja instalar. Por padrão, são selecionados todos os componentes do Antivírus de arquivos, o componente de verificação de vírus e o conector de Agente de rede para gerenciar o aplicativo em forma remota por meio do Kit de Administração Kaspersky.

Para selecionar um componente para continuar a instalação, deve abrir o menu clicando no botão esquerdo no ícone ao lado do nome do componente e selecionar. **Este recurso será instalado no disco rígido local**. A parte inferior da janela do programa de instalação exibe a informação sobre qual tipo de proteção é fornecida pelo componente selecionado e quanto espaço de armazenamento é necessário para sua instalação.

Para conhecer informação detalhada sobre o espaço disponível em disco no seu computador, clique no botão **Volume**. A informação aparecerá na janela que será aberta.

Para cancelar a instalação de componentes, selecione **Este recurso não estará disponível** no menu de contexto. Se você cancelar a instalação de algum componente, não estará protegido contra uma série de programa perigosos.

Quando terminar de selecionar os componentes que serão instalados, clique no botão **Avançar.** Para voltar à lista padrão de componentes por instalar, clique no botão **Reiniciar.**

ETAPA 9. PESQUISA DE OUTROS APLICATIVOS ANTIVÍRUS

Nesta etapa, o assistente pesquisa outros programas antivírus, incluídos outros programas da Kaspersky Lab, que possam estar em conflito com o Kaspersky Anti-Virus.

Se algum aplicativo antivírus for detectado no seu servidor, será enumerado na tela. Você terá a opção de desinstalar esses programas antes de proceder com a instalação.

Você pode escolher entre removê-los automaticamente ou manualmente, usando os controles localizados abaixo da lista de programas antivírus detectados (Somente os produtos da Kaspersky Lab serão excluídos automaticamente).

Para proceder com a instalação, clique no botão **Avançar.**

ETAPA 10. PREPARAÇÃO FINAL PARA A INSTALAÇÃO

Esta etapa completa a preparação para instalar o aplicativo no seu servidor.

Na instalação inicial do Kaspersky Anti-Virus 6.0, é recomendável não desmarcar a caixa ☑ **Proteger do processo de instalação**. A ativação da proteção dos módulos permite executar o procedimento correto de reversão da instalação se houver erros durante a instalação do aplicativo. Quando tentar novamente a instalação de um aplicativo, é recomendável desmarcar esta caixa.

Se o aplicativo é instalado remotamente usando o **Windows Remote Desktop**, é recomendável desmarcar a caixa ☑ **Proteger o processo de instalação**. Caso contrário, o procedimento de instalação pode ser executado incorretamente ou ficar incompleto.

Se desejar que as exclusões recomendadas pela Microsoft sejam adicionadas automaticamente à lista de exclusões, marque a caixa ☑ **Excluir da verificação antivírus as áreas recomendadas pela Microsoft**.

Se você quer adicionar o caminho avp.com à variável ambiental %Path% depois da instalação, marque a caixa ☑ **Adicionar o caminho de avp.com à variável do sistema %PATH%**.

Para proceder com a instalação, clique no botão **Instalar**.

Quando instalar os componentes do Kaspersky Anti-Virus, que interceptam o tráfego da rede, as conexões das redes atuais são encerradas. A maioria das conexões encerradas é reiniciada depois de algum tempo.

ETAPA 11. CONCLUSÃO DA INSTALAÇÃO

A janela de **Instalação completa** contém informações sobre como completar a instalação do Kaspersky Anti-Virus no seu computador.

Para executar o Auxiliar de Configuração inicial, clique no botão **Avançar**.

Se for necessário reiniciar para completar a instalação com êxito, a notificação especial aparecerá na tela.

INSTALAÇÃO DO APLICATIVO A PARTIR DA LINHA DE COMANDO

➡ *Para instalar o Kaspersky Anti-Virus 6.0 para Windows Servers MP4, digite o seguinte na linha de comando:*

```
msiexec /i <nome_pacote>
```

O assistente de instalação será executado (ver seção "Instalação usando o Assistente de instalação" na página 16). Quando o aplicativo for instalado, é necessário reiniciar.

- *Para instalar o aplicativo em modo não interativo (sem executar o assistente de instalação), digite o seguinte:*

```
msiexec /i <nome do pacote> /qn
```

Neste caso, o computador deve ser reiniciado manualmente quando a instalação do aplicativo estiver completa. Para reiniciar o computador automaticamente, digite o seguinte na linha de comando:

```
msiexec /i <nome do pacote> ALLOWREBOOT=1 /qn
```

Leve em conta que a reinicialização automática somente pode ser feita no modo de instalação não interativo (com a tecla /qn).

- *Para instalar o aplicativo com uma senha, que confirma o direito a remover o aplicativo, digite o seguinte:*

`msiexec /i <package_name> KLUNINSTPASSWD=******` – ao instalar o aplicativo em modo interativo;

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=****** /qn` – quando instalar o aplicativo em um modo não interativo sem reiniciar o computador;

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn` – quando instalar o aplicativo em um modo não interativo e depois reiniciar o computador.

Quando instalar o Kaspersky Anti-Virus em modo não interativo, a leitura do arquivo setup.ini é compatível. O arquivo contém configurações gerais para a instalação do aplicativo, o arquivo de configuração *install.cfg* (ver seção Importar configurações de proteção na página 108) e o arquivo da chave da licença. Leve em conta que esses arquivos devem estar localizados na mesma pasta que o pacote de instalação do Kaspersky Anti-Virus.

INSTALAÇÃO DESDE O EDITOR DO OBJETO DE POLÍTICA DE GRUPO

Usando o **Editor do objeto de política de grupo**, você pode instalar, atualizar e remover o Kaspersky Anti-Virus nas estações de trabalho da empresa que formam parte do domínio, sem usar o Kit de Administração Kaspersky.

INSTALAÇÃO DO APLICATIVO

- *Para instalar o Kaspersky Anti-Virus:*

1. Criar uma pasta de rede compartilhada no computador, que funciona comocontrolador de domínio, e colocar o pacote de instalação do Kaspersky Anti-Virus em formato *MSI* dentro dela.

   Além disso, neste diretório você pode colocar o arquivo *setup.ini*, que contém um lista de configurações para a instalação do Kaspersky Anti-Virus, o arquivo de configuração *install.cfg* (ver seção Importar configurações de proteção na página 108) e o arquivo de chave da licença.

2. Abra o **editor do Objeto de política de grupo** da consola MMC padrão (para obter informação detalhada sobre como trabalhar com este editor, consulte o sistema de ajuda do Microsoft Windows Server).

3. Crie um novo pacote. Para isso, selecione o **Objeto da política de grupo / configuração do computador/ configuração do programa / instalação do software** desde a árvore da consola e use o comando **Criar / Pacote** desde o menu de contexto.

   Na janela que será aberta, especifique o caminho até a pasta de rede compartilhada que armazena o pacote de instalação do Kaspersky Anti-Virus. Na caixa de diálogo de **Implantação do programa**, selecione a Configuração **atribuída** e clique no botão **OK**.

A política do grupo será aplicada a cada estação de trabalho no próximo registro de computadores no domínio. Como resultado, o Kaspersky Anti-Virus será instalado em todos os computadores.

DESCRIÇÃO DAS CONFIGURAÇÕES DO ARQUIVO SETUP.INI

O arquivo *setup.ini* localizado no diretório do pacote de instalação do Kaspersky Anti-Virus é usado para instalar o aplicativo em modo não interativo desde a linha de comando ou o editor do Objeto de política de grupo. O arquivo inclui as seguintes configurações:

[Setup] – configurações gerais para a instalação do aplicativo.

- **InstallDir=**<caminho até a pasta de instalação do aplicativo>.
- **Reboot=sim|não** – define se o computador deve ser reiniciado ou não quando a instalação do aplicativo estiver completa (a reinicialização não é executada por padrão).
- **SelfProtection=sim|não** – define se a Autodefesa do Kaspersky Anti-Virus deve ser ativada durante a instalação (a Autodefesa está ativada por padrão).

[Componentes] – seleção dos componentes do aplicativo a serem instalados. Se este grupo não conter componentes, o aplicativo será instalado totalmente.

- **FileMonitor=sim|não** – Instalação do componente Antivírus de arquivo.

[Tarefas] – Ativação das tarefas do Kaspersky Anti-Virus. Se nenhuma das tarefas for especificada, todas as tarefas estarão ativadas após a instalação. Se pelo menos uma tarefa estiver especificada, as tarefas que não foram enumeradas serão desabilitadas.

- **ScanMyComputer=sim|não** – Tarefa de verificação completa.
- **ScanStartup=sim|não** – Tarefa de verificação rápida.
- **Scan=sim|não** – Tarefa de verificação.
- **Updater=sim|não** – Tarefa de atualização para os bancos de dados dos aplicativos e os módulos do programa.

Os valores 1, ligado, ativar e ativado podem ser usados no lugar do valor **sim**. Os valores 0, desligado, desativar e desativado podem ser usados no lugar do valor **não**.

ATUALIZANDO A VERSÃO DO APLICATIVO

Para atualizar a versão do Kaspersky Anti-Virus:

1. Coloque o pacote de instalação que contém as atualizações do Kaspersky Anti-Virus em formato .msi em uma pasta de rede compartilhada.
2. Abra o **editor do Objeto de política do grupo** e crie um novo pacote usando o procedimento descrito acima.
3. Selecione o novo pacote da lista e use o comando **Propriedades** no menu de contexto. Selecione a aba **Atualizações** na janela de propriedades do pacote e especifique o pacote, que contém o pacote de instalação da versão anterior do Kaspersky Anti-Virus. Para instalar uma versão atualizada do Kapersky Anti-Virus salvando as configurações de proteção selecione a opção de instalação sobre o pacote existente.

A política do grupo será aplicada a cada estação de trabalho no próximo registro de computadores no domínio.

Leve em conta que os computadores que funcionam com Microsoft Windows 2000 Server não são compatíveis com a atualização do Kaspersky Anti-Virus por meio do editor de Objetos de política de grupos.

EXCLUSÃO DO APLICATIVO

➡ *Para excluir o Kaspersky Anti-Virus:*

1. Abra o **Editor do Objeto de política do grupo**.
2. Selecione **Objeto_Política_Grupo /Configuração do computador/Configuração do programa/ Instalação do software** na árvore do console.

   Selecione o pacote do Kaspersky Anti-Virus da lista de pacotes, abra o menu de contexto e execute o comando **Todas as tarefas/ Excluir**.

Na caixa de diálogo **Excluindo aplicativos**, selecione **Excluir imediatamente este aplicativo dos computadores de todos os usuários** para que o Kaspersky Anti-Virus seja excluído na próxima reinicialização.

GUIA RÁPIDO

Um dos principais objetivos da Kaspersky Lab ao criar o Kaspersky Anti-Virus foi fornecer o aplicativo com uma configuração ideal.

Para a conveniência do usuário, reunimos os estágios de configuração preliminares na interface unificada do Assistente de Configuração Inicial que é iniciado ao concluir o procedimento de instalação do aplicativo. Seguindo as instruções do Assistente, você pode ativar o programa, configurar as configurações para executar atualizações e tarefas de verificação de vírus, acesso protegido por senha ao aplicativo.

Depois de concluir a instalação e de iniciar o programa, é recomendável fazer o seguinte:

- Avaliação do status de proteção atual (ver seção "Gerenciamento de segurança" na página 29) para verificar que o Kaspersky Anti-Virus assegure o nível apropriado de segurança.
- Atualização do aplicativo (ver seção atualização do aplicativo na página 28) (caso ela não tenha sido executada usando o Assistente de configuração ou automaticamente, imediatamente após a instalação do aplicativo).
- Verificação de vírus no servidor (ver seção "Verificando vírus no computador" na página 27).

NESTA SEÇÃO

ASSISTENTE DE CONFIGURAÇÃO INICIAL

O Assistente de configuração do Kaspersky Anti-Virus inicia-se ao finalizar a instalação do aplicativo. Ele foi criado para ajudá-lo a configurar as configurações iniciais do aplicativo com base nos recursos e tarefas do computador.

A interface do Assistente de configuração está desenhada como um Assistente padrão do Microsoft Windows e inclui uma série de etapas que você pode procurar usando os botões **Avançar** e **Voltar**, ou completar usando o botão **Concluir**. Para interromper o assistente a qualquer etapa, use o botão **Cancelar**.

Para completar a instalação do aplicativo no computador, todas as etapas do procedimento do assistente devem ser completadas. Se a operação do assistente for interrompida por algumas razões, os valores das configurações já especificadas não serão salvos. Na próxima tentativa de executar o aplicativo o Assistente de configuração inicial é executado novamente e exige a reedição das configurações.

USO DOS OBJETOS SALVOS DA VERSÃO ANTERIOR

Esta janela do assistente aparecerá quando você instalar o aplicativo sobre a versão anterior do Kaspersky Anti-Virus. Você pode escolher quais dados da versão anterior devem ser importados para a nova versão. Estes dados podem incluir objetos em quarentena ou salvos como backup ou configurações de segurança.

Para usar esses dados na nova versão do aplicativo marque todas as caixas necessárias.

ATIVANDO O APLICATIVO

O procedimento de ativação do aplicativo consiste em registrar uma licença através da instalação de um arquivo de chave. O aplicativo determinará os privilégios existentes e calculará seu prazo de uso de acordo com a licença.

O arquivo de chave contém as informações dos serviços necessárias para o funcionamento total do Kaspersky Internet Anti-Virus, além de dados adicionais:

- informações de suporte (quem fornece o suporte e onde é possível obtê-lo);
- nome e número da chave e a data de expiração da licença.

Dependendo de se você já tem um arquivo de chave ou se receberá um arquivo do servidor da Kaspersky Lab, você tem as seguintes opções para ativar o Kaspersky Anti-Virus:

- Ativação online (veja página 25). Selecione esta opção de ativação se tiver comprado uma versão comercial do aplicativo e recebido um código de ativação. Você pode usar este código para obter um arquivo de chave que forneça acesso à funcionalidade completa do aplicativo ao longo do prazo de vigência da licença.
- Ativação da versão de avaliação (veja página 25). Use esta opção de ativação se desejar instalar a versão de avaliação do aplicativo antes de decidir comprar a versão comercial. Você receberá um arquivo de chave gratuito válido pelo período especificado no contrato de licença da versão de avaliação.
- Ativação com um arquivo de chave de licença obtido anteriormente (veja seção "Ativação usando um arquivo de chave" na página 25). Ative o aplicativo usando a chave do Kaspersky Anti-Virus 6.0 obtido anteriormente.
- Ativação posterior. Se você selecionar esta opção, ignorará a etapa de ativação. Este aplicativo será instalado no seu computador e você terá acesso a todas as funções do aplicativo, exceto para as atualizações (apenas uma atualização de aplicativo estará disponível e será imediatamente após a instalação). A opção **Ativar mais tarde** estará disponível somente ao iniciar o Assistente de ativação pela primeira vez. Nas demais execuções do assistente, se o aplicativo já estiver ativado, a opção **Excluir o arquivo de chave** estará disponível para realizar a exclusão.

Se alguma das duas primeiras opções de ativação de aplicativos estiver selecionada, o aplicativo será ativado por meio do servidor da Kaspersky Lab, que requer uma conexão com a Internet para ser acessado. Antes de iniciar a ativação, verifique e edite as configurações de conexão com a rede conforme solicitado na janela que será aberta clicando no botão **Configurações da LAN**. Para obter mais detalhes sobre as configurações da rede, comunique-se com o administrador da rede ou o provedor de Internet.

Se no momento da instalação não houver conexão com a Internet disponível, você pode fazer a ativação mais tarde, usando a interface do aplicativo ou conectando-se com a Internet através de um computador diferente e obtendo uma chave, usando um código de ativação recebido através de registro no site de Serviço de Suporte Técnico da Kaspersky Lab.

Você também pode ativar o aplicativo usando o Kit de Administração Kaspersky. Para isso, você deve criar uma tarefa de instalação do arquivo de chave (veja página 123) (para obter mais detalhes, consulte a guia de ajuda do Kit de Administração Kaspersky).

CONSULTE TAMBÉM:

ATIVAÇÃO ONLINE

A ativação online é executada inserindo o código de ativação que você recebeu por email ao comprar o Kaspersky Anti-Virus pela Internet. Se você comprou o aplicativo em uma caixa (versão de varejo), o código de ativação estará impresso no envelope que contém o disco de instalação.

INSERINDO O CÓDIGO DE ATIVAÇÃO

Nesta etapa, o código de ativação deve ser inserido. O código de ativação é uma sequência de números e letras separados por hífens em quatro grupos de cinco símbolos, sem espaços. Por exemplo, 11111-11111-11111-11111. Observe que o código somente deve ser inserido em caracteres latinos.

Digite sua informação pessoal na parte inferior da janela: nome e sobrenome, endereço de email, país e cidade de residência. Esta informação pode ser necessária para identificar um usuário registrado se, por exemplo, seus dados de licença forem perdidos ou roubados. Neste caso, você pode obter outro código de ativação usando sua informação pessoal.

OBTENDO UM ARQUIVO DE CHAVE

O Assistente de configuração conecta-se aos servidores de Internet da Kaspersky Lab e envia seus dados de registro, incluídos o código de ativação e suas informações de contato. Uma vez estabelecida a conexão, o código de ativação e as informações de contato serão verificadas. Se o código de ativação passar na verificação, o assistente receberá um arquivo de chave que será instalado automaticamente. Ao terminar a ativação, a janela com informações detalhadas sobre a licença obtida será aberta.

Se o código de ativação não for aprovado pela verificação, você verá um aviso pop-up correspondente na tela. Se isto acontecer, comunique-se com o fornecedor de software de quem você comprou o aplicativo para obter informação.

Se o número de ativações permitidas para esse código tiver sido excedido, o aviso pop-up correspondente será exibido na tela. O processo de ativação será interrompido e você poderá entrar em contato com o serviço de Suporte técnico da Kaspersky Lab.

ATIVANDO A VERSÃO TESTE

Use esta opção de ativação se desejar instalar a versão teste do Kaspersky Anti-Virus antes de decidir comprar a versão comercial. Você receberá uma licença gratuita que será válida pelo período especificado no contrato de licença da versão teste. Uma vez vencida a licença, você não poderá ativar novamente a versão teste.

ATIVAÇÃO USANDO UM ARQUIVO DE CHAVE

Se você tiver um arquivo de chave poderá usá-lo para ativar o Kaspersky Anti-Virus. Para fazê-lo, use o botão **Procurar** e selecione o caminho do arquivo com extensão *.key*.

Depois da instalação bem-sucedida da chave, você verá as informações sobre a licença na parte inferior da janela: número da licença, tipo de licença (comercial, de avaliação, etc.), data de expiração e número de hosts.

CONCLUIR A ATIVAÇÃO

O Assistente de configuração o informará que a ativação do Kaspersky Anti-Virus foi bem-sucedida. Além disso, são fornecidas as informações sobre a licença: número da licença, tipo (comercial, de avaliação, etc.), data de expiração e número de hosts.

ATUALIZAR A CONFIGURAÇÃO DAS CONFIGURAÇÕES

A qualidade da proteção do computador depende diretamente da atualização periódica dos bancos de dados e dos módulos do aplicativo. Nesta janela o Assistente de configuração solicita que você selecione o modo de atualização do aplicativo e edite as configurações do agendamento:

- **Automaticamente**. O Kaspersky Anti-Virus verifica a fonte de atualização para pacotes de atualização em intervalos especificados. A frequência de verificação pode aumentar durante o uso do antivírus e diminuir quando estão concluídos. Se novas atualizações são encontradas, o Kaspersky Anti-Virus as descarrega e instala no computador. Este é o modo padrão.
- **A cada 2 horas** (a frequência pode variar dependendo das configurações de programação). As atualizações serão executadas automaticamente de acordo com a programação criada. Você pode modificar as configurações de programação em outra janela clicando no botão **Alterar**.
- **Manualmente**. Ao selecionar esta opção, você mesmo executará as atualizações do aplicativo.

Os bancos de dados e módulos do aplicativo fornecidos com o pacote de instalação podem estar desatualizados no momento da instalação do aplicativo. Por isso é recomendável obter as últimas atualizações do aplicativo. Para fazê-lo, clique no botão **Atualizar agora**. Então o Kaspersky Anti-Virus baixará as atualizações necessárias dos sites de atualização e os instalará no computador.

Se você desejar mudar para atualizações de configuração (especificar configurações de rede, selecionar uma fonte de atualização, executar uma atualização de uma conta de usuário específica ou ativar a baixa de atualização a uma fonte local), clique no botão **Configurações**.

CONFIGURAR A PROGRAMAÇÃO DE VERIFICAÇÃO DE VÍRUS

Verificar as áreas selecionadas para detectar objetos maliciosos é uma das tarefas principais para proteger seu computador.

Quando instalar o Kaspersky Anti-Virus, três tarefas padrão de verificação de vírus são criadas. Nesta janela, o Assistente de configuração solicita que selecione um modo para executar a tarefa de verificação:

Verificação completa

Uma verificação completa de todo o sistema. Os seguintes objetos são verificados por padrão: memória do sistema, programas carregados na inicialização, backup do sistema, bancos de dados de email, discos rígidos, mídias de armazenamento removíveis e unidades de rede. Você pode modificar as configurações de programação na janela que será aberta ao clicar no botão **Alterar**.

Verificação rápida

Verificação de vírus nos objetos de inicialização do sistema operacional. Você pode modificar as configurações de programação na janela que será aberta ao clicar no botão **Alterar**.

RESTRIÇÃO DO ACESSO AO APLICATIVO

Como um servidor pode ser usado por várias pessoas com diferentes níveis de conhecimentos de informática e como o malware pode desativar a proteção do computador, você tem a opção de restringir o acesso ao Kaspersky Anti-Virus usando uma senha. O uso de uma senha pode proteger o aplicativo das tentativas não autorizadas de desativar a proteção, alterar as configurações ou desinstalar o aplicativo.

Para ativar a proteção por senha, selecione a caixa ☑ **Ativar proteção por senha** e preencha os campos **Senha** e **Confirmar senha**.

Especifique a seguir a área que deseja proteger com a senha:

- ◉ **Todas as operações (exceto notificações de eventos perigosos)**. A senha será solicitada se o usuário tentar executar qualquer ação com o aplicativo, exceto responder notificações sobre a detecção de objetos perigosos.
- ◉ **Operações selecionadas**:
  - ☑ **Configurando o aplicativo** – a senha será solicitada se um usuário tentar modificar as configurações do Kaspersky Anti-Virus.
  - ☑ **Fechando o aplicativo** – a senha será solicitada quando o usuário tentar sair do aplicativo.
  - ☑ **Desativando componentes de proteção e interrompendo tarefas de verificação** – a senha será solicitada quando o usuário tentar desativar o Antivírus de arquivos ou interromper uma tarefa de verificação de vírus.
  - ☑ **Desativando a diretiva do Kaspersky Administration Kit** – a senha será solicitada se o usuário tentar remover o computador do escopo das diretivas e tarefas de grupos (ao trabalhar com o Kaspersky Administration Kit).
  - ☑ **Ao desinstalar o aplicativo** – a senha será solicitada se o usuário tentar remover o aplicativo do computador.

ENCERRANDO O ASSISTENTE DE CONFIGURAÇÃO

Na última janela do assistente, você verá uma mensagem que indica que o Kaspersky Anti-Virus foi instalado e configurado com êxito. Você pode iniciar o aplicativo imediatamente marcando ☑ **Iniciar o aplicativo**.

Se houver algum problema durante a instalação, como um problema de incompatibilidade com outros aplicativos antivírus, você deverá reiniciar seu computador.

VERIFICANDO VÍRUS NO COMPUTADOR

Os desenvolvedores de malware se empenham em ocultar suas ações; assim, talvez você não note a presença de programas de malware no seu computador.

Depois do Kaspersky Anti-Virus ser instalado no seu computador, ele automaticamente executa a tarefa de **Verificação rápida** no seu computador. Esta tarefa pesquisa e neutraliza programas perigosos em objetos carregados durante a inicialização do sistema operacional.

Os especialistas da Kaspersky Lab também recomendam que você execute a tarefa de **Verificação completa**.

➡ *Para iniciar/interromper uma tarefa de verificação de vírus:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Clique no botão **Iniciar verificação** para iniciar o processo de verificação. Se você precisar interromper a execução da tarefa, clique no botão **Interromper verificação** enquanto a tarefa estiver em andamento.

ATUALIZANDO O APLICATIVO

É necessário ter uma conexão com a Internet para atualizar o Kaspersky Anti-Virus.

O pacote de instalação do Kaspersky Anti-Virus inclui os bancos de dados, que contêm assinaturas de ameaças. No momento em que é instalado o aplicativo, esses bancos de dados podem resultar obsoletas, já que a Kaspersky Lab atualiza os bancos de dados e os módulos dos aplicativos em forma regular.

Quando o Assistente de configuração inicial está ativo, é possível selecionar o modo de execução da atualização. Por padrão, o Kaspersky Anti-Virus verifica automaticamente as atualizações nos servidores da Kaspersky Lab. Se o servidor contém um grupo novo de atualizações, o Kaspersky Anti-Virus o descarregará e instalará no modo silencioso.

Para manter a proteção de seu computador atualizada, é recomendável atualizar o Kaspersky Anti-Virus imediatamente após a instalação.

Para atualizar o Kaspersky Anti-Virus em forma independente:

1. Abra a janela principaldo aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Clique no botão **Iniciar atualização**.

GERENCIAMENTO DE LICENÇAS

O Kaspersky Anti-Virus requer uma licença para operar. Você recebe uma licença quando compra o produto. Esta licença lhe dá o direito de usar o produto assim que for ativado.

Sem a licença, se a versão de avaliação do aplicativo não foi ativada, o Kaspersky Anti-Virus funcionará em modo Uma atualização. O aplicativo não baixará novas atualizações.

Se a versão de avaliação do aplicativo foi ativada, o Kaspersky Anti-Virus não funcionará depois de expirar a licença gratuita.

Quando a licença comercial expirar, o programa continuará funcionando, mas você não poderá atualizar seus bancos de dados. Como antes, você poderá verificar seu computador quanto à presença de vírus e usar os componentes de proteção, mas apenas com os bancos de dados que você tinha antes de a licença expirar. Não podemos garantir que você estará protegido contra os vírus que surgirem depois da expiração da licença do programa.

Para não infetar seu computador com novos vírus, é recomendável renovar sua licença do Kaspersky Anti-Virus. Duas semanas antes do vencimento da licença, o aplicativo lhe notifica sobre o vencimento . Durante algum tempo, uma mensagem correspondente será exibida sempre que o aplicativo for iniciado.

As informações gerais sobre a licença atualmente em uso (licenças ativas e adicionais se a última foi instalada) são exibidas na seção **Licença** da janela principal do Kaspersky Anti-Virus: Tipo de licença (completa, avaliação, beta), número máximo de anfitriões, data de expiração da licença e número de dias até a data de expiração. Para obter mais detalhes sobre a licença, clique no link com o tipo de licença atualmente em uso.

Para exibir os termos do contrato de licença do aplicativo, clique no botão **Exibir Contrato de licença do usuário final**.

Para eliminar a licença, clique no botão **Adicionar** / **Excluir** e siga as instruções do assistente que será aberto.

A Kaspersky Lab oferece preços promocionais para as renovações de licenças de nossos produtos. Verifique as ofertas especiais no site da Kaspersky Lab.

➧ *Para comprar ou renovar uma licença:*

1. Comprar um novo arquivo de chave ou um código de ativação. Use o botão **Comprar licença** (se o aplicativo não for ativado) ou **Renovação da licença**. Na página da Web que será aberta, serão exibidas informações detalhadas sobre os termos de compra da chave na Loja virtual da Kaspersky Lab ou de distribuidores autorizados. Se você comprar online, um arquivo de chave ou um código de ativação serão enviados por email para o endereço especificado no formulário do pedido, assim que o pagamento for efetuado.

2. Ativar o aplicativo. Use o botão **Adicionar /Excluir** chave na seção **Licença** da janela principal do aplicativo ou use o comando **Ativação** no menu de contexto do aplicativo. O Assistente de ativação será iniciado.

GERENCIAMENTO DE SEGURANÇA

Os problemas na proteção do computador são indicados pelo status de proteção do computador (veja seção "Janela principal do aplicativo" na página 34), que é exibida com mudanças da cor no ícone de proteção do computador no painel onde está localizado. Quando aparecem problemas de proteção, é recomendável resolvê-los.

Figura 1. Status de proteção atual do computador

Você pode ver a lista de problemas ocorridos, sua descrição e as formas possíveis de resolvê-los, por mio do Assistente de segurança (ver figura abaixo), que pode ser ativado clicando no link **Corrigir** (ver figura abaixo).
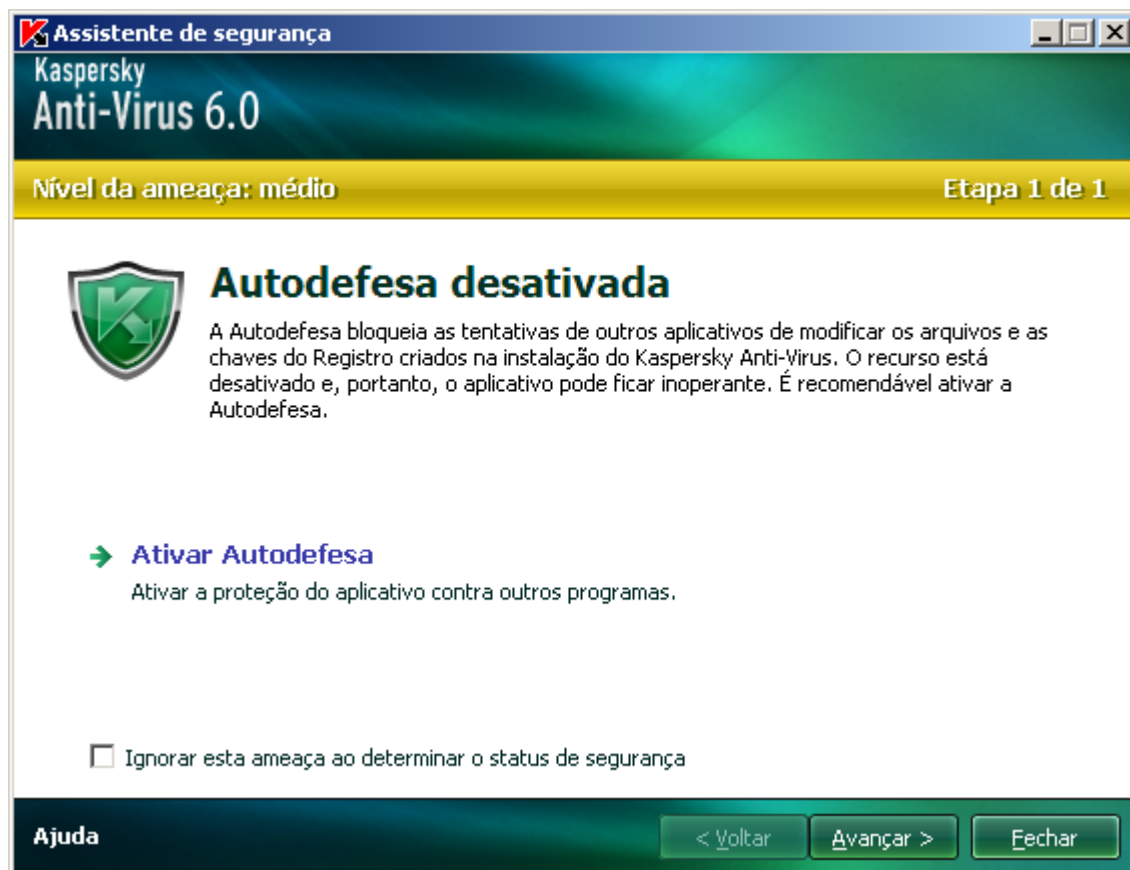
Figura 2. Solução de problemas de segurança

Você pode ver a lista dos problemas atuais. Os problemas são classificados de acordo com sua importância: primeiro os problemas mais críticos (com o ícone de status vermelho), então os menos importantes, com o ícone de status amarelo, e finalmente – as mensagens informativas. É fornecida uma descrição detalhada de cada problema, e as seguintes ações estão disponíveis:

- *Eliminar imediatamente*. Usando os links correspondentes, você pode alternar para a correção do problema, que é a ação recomendada.
- *Adiar a eliminação*. Se, por algum motivo, a eliminação imediata do problema não for possível, você poderá adiar essa ação e voltar a ela mais tarde. Marque a caixa ☑ **Ignorar esta ameaça ao determinar o status de segurança** para que a ameaça não afete o status atual de proteção.

  No caso de problemas graves, essa opção não estará disponível. Esses problemas incluem, por exemplo, objetos perniciosos que não foram desinfetados, interrupção de um ou de vários componentes ou corrupção dos arquivos do aplicativo. Os problemas como este devem ser eliminados o mais rápido possível.

PAUSAR A PROTEÇÃO

Pausar a proteção consiste em desativar temporalmente o Antivírus de arquivos.

➡ *Para pausar o Kaspersky Anti-Virus:*

1. No menu de contexto do aplicativo, selecione o item **Pausar proteção**.
2. Na janela **Pausar a proteção** que será aberta, selecione o período durante o qual você deseja ativar a proteção, das opções sugeridas.

ELIMINAÇÃO DE PROBLEMAS. SUPORTE TÉCNICO AO USUÁRIO

Se houver problemas com a operação do Kaspersky Anti-Virus, o primeiro lugar para procurar ajuda e resolver o problema é o Sistema de ajuda. O segundo lugar é o Banco de dados de conhecimentos da Kasperky Lab (http://usa.kaspersky.com/support/corporate/). A *Banco de dados de conhecimento* é uma seção independente do site de Suporte técnico, com recomendações referentes aos produtos da Kaspersky Lab e respostas às perguntas mais frequentes. Tente usar esse recurso para encontrar uma resposta à sua dúvida ou uma solução para seu problema.

➡ *Para usar o Banco de dados de conhecimentos:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no link **Suporte**.
3. Na janela **Suporte** que será aberta, clique no link **Serviço de Suporte técnico**.

Outro recurso que você pode usar para obter informações sobre como trabalhar com o aplicativo é o Fórum de usuários da Kaspersky Lab. Ele consiste em outra seção independente do site de Suporte técnico e contém perguntas, comentários e solicitações de usuários. Você pode exibir os temas principais, deixar comentários ou encontrar a resposta para uma pergunta.

➡ *Para abrir o Fórum de usuários:*

1. Abra o janela principal do aplicativo.
2. Na parte inferior da janela, clique no link **Suporte**.
3. Na janela **Suporte** que será aberta, clique no link **Fórum de usuários**.

Se não conseguir encontrar uma solução para seu problema na Ajuda, no Banco de dados de conhecimento ou no Fórum de usuários, entre em contato com o Suporte técnico da Kaspersky Lab.

CRIANDO UM ARQUIVO DE RASTREAMENTO

Depois de instalar o Kaspersky Anti-Virus, podem ocorrer algumas falhas no sistema operacional ou na operação de aplicativos individuais. A causa mais provável é um conflito entre o aplicativo e o software instalado no computador, ou com os drivers dos componentes do computador. Talvez seja solicitado que você crie um arquivo de rastreamento para que os especialistas da Kaspersky Lab possam solucionar seu problema.

Para criar o arquivo de rastreamento:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no link **Suporte**.
3. Na janela **Suporte** que será aberta, clique no link **Rastros**.
4. Na janela **Informação para o serviço de suporte técnico** que será aberta, use a lista suspensa na seção **Rastros** para selecionar o nível de rastreamento. O nível de rastreamento deve ser definido de acordo com a recomendação do especialista de Suporte técnico. Se não houver indicações do Suporte técnico, é recomendável definir o nível de rastreamento como **500**.
5. Para iniciar o processo de rastreamento, clique no botão **Ativar**.
6. Reproduza a situação que causou o problema.
7. Para interromper o processo de rastreamento, clique no botão **Desativar**.

CONFIGURAÇÃO DAS CONFIGURAÇÕES DO APLICATIVO

A janela de configurações do aplicativo (veja página 70), que pode ser acessada da janela principal clicando no botão **Configurações**, está desenhada para o acesso rápido às configurações do Kaspersky Anti-Virus 6.0.

RELATÓRIOS DE OPERAÇÃO DO APLICATIVO. ARQUIVOS DE DADOS

A operação do Antivírus de arquivos e o desempenho de cada tarefa de verificação de vírus e atualização são registrados em um relatório (veja página 85). Para ver relatórios, use o botão **Relatórios** no canto direito inferior da janela principal.

Os objetos colocados em quarentena (veja página 86) ou na cópia de backup (veja página 87) pelo Kaspersky Anti-Virus são chamados *arquivos de dados*. Clicando no botão **Detectado**, você pode abrir a janela **Armazenamento**, onde poderá realizar qualquer ação que quiser nestes objetos.

INTERFACE DO APLICATIVO

O Kaspersky Anti-Virus possui uma interface simples e fácil de usar. Este capítulo destaca suas características básicas:

- ícone na bandeja do sistema;
- menu de contexto;
- janela principal;
- notificações;
- janela de configuração do Kaspersky Anti-Virus.

NESTA SEÇÃO

ÍCONE DA ÁREA DE NOTIFICAÇÃO DA BARRA DE TAREFAS

Depois de instalar o Kaspersky Anti-Virus, seu ícone aparecerá na bandeja do sistema.

O ícone é um tipo de indicador para as operações do Kaspersky Anti-Virus. Ele também reflete o status da proteção e mostra várias funções básicas executadas pelo aplicativo.

Se o ícone está ativo (com cor), significa que a proteção está ativada no servidor. Se o ícone está inativo (branco e preto), significa que a proteção está desativada.

O ícone do Kaspersky Anti-Virus muda de acordo com a operação do programa em execução:

– verificação de um arquivo que você ou algum programa está abrindo, salvando ou executando.

– a atualização do banco de dados do Kaspersky Anti-Virus e do módulo está em andamento.

– ocorreu um erro na operação de algum componente do Kaspersky Anti-Virus.

O ícone também dá acesso aos componentes básicos da interface do aplicativo: menu de contexto e janela principal.

Para abrir o menu de contexto, clique com o botão direito do mouse no ícone do aplicativo.

Para abrir a janela principal do Kaspersky Anti-Virus, clique no ícone do aplicativo.

MENU DE CONTEXTO

Você pode executar as tarefas de proteção básicas no menu de contexto, que contêm estes itens:

- **Verificação completa** – inicia uma verificação completa do computador para detectar objetos maliciosos. Os objetos que residem em todas as unidades, incluindo mídias de armazenamento removíveis, serão verificados.
- **Scan –** seleciona objetos e inicia a verificação de vírus. Por padrão, a lista contém uma série de objetos, como a memória do sistema, objetos de início, bancos de dados de emails, todas as unidades de servidor etc. Você pode ampliar a lista, selecionar outros objetos para verificar e começar a verificação de vírus.
- **Atualizar –** inicia as atualizações para os módulos do aplicativo e os bancos de dados do Kaspersky Anti-Virus e os instala no seu computador.
- **Ativar** – ativa o aplicativo. Para ser um usuário registrado com acesso à funcionalidade completa do aplicativo e o Suporte técnico, você tem que ativar sua versão do Kaspersky Anti-Virus. Este item de menu estará disponível somente se o aplicativo não tiver sido ativado.
- **Configurações** – visualiza e edita configurações do Kaspersky Anti-Virus.
- **Kaspersky Anti-Virus –** abre a janela principal do aplicativo.
- Pausar **/ Reiniciar a proteção –** ativa ou desativa temporalmente o Antivírus de arquivos. Essa opção do menu não afeta as atualizações do aplicativo ou a execução das verificações de vírus.
- **Desativar política /Ativar política –** desativa ou ativa temporalmente a política quando o aplicativo trabalha por meio do Kit de Administração Kaspersky. Este item do menu permite remover o computador do escopo das políticas e das tarefas de grupo. Esta oportunidade é gerenciada com uma senha (ver seção "Restrição de acesso ao aplicativo" na página 80). O item do menu somente aparece se uma senha é definida.
- **Sobre** – exibe uma janela com informações do aplicativo.
- **Sair –** fecha o Kaspersky Anti-Virus (ao selecionar essa opção, o aplicativo será descartado da RAM do computador).
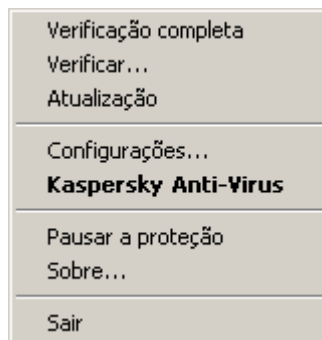
Figura 3. Menu de contexto

Se uma tarefa de verificação de vírus está sendo executada, seu nome será exibido no menu de atalhos com uma indicação da percentagem de andamento. Depois de selecionar uma tarefa, você pode ir para janela de relatórios para ver os resultados atuais de desempenho.

JANELA PRINCIPAL DO APLICATIVO

A janela principal do aplicativo pode ser dividida em três partes:

- A parte superior da janela indica o status de proteção atual do computador.

Figura 4. Status de proteção atual do computador

Há três valores possíveis de status de proteção: cada um deles é indicado por uma determinada cor, de forma semelhante às luzes de sinalização de tráfego. O verde indica que a proteção do seu computador está no nível correto, enquanto amarelo e vermelho indicam que há ameaças de segurança na configuração do sistema ou na operação do Kaspersky Anti-Virus. Além dos programas maliciosos, as ameaças incluem, por exemplo, bancos de dados desatualizados de aplicativos.

As ameaças de segurança devem ser eliminadas assim que aparecerem. Para obter informações detalhadas sobre elas e eliminá-las rapidamente, use o link **Corrigir** (veja a figura acima).

- A parte esquerda da janela oferece o acesso rápido para qualquer função do aplicativo, incluídas as tarefas de verificação de vírus, atualizações, etc.

Figura 5. Parte esquerda da janela principal

- À direita da janela, existem informações sobre a função do aplicativo selecionada à esquerda, sendo possível definir suas configurações, com ferramentas para a execução de tarefas de verificação de vírus, recuperação de atualizações, etc.

Figura 6. Parte direita da janela principal

Além disso, você pode usar as seguintes opções:

- O botão **Configurações** - para abrir a janela de configuração (veja página 70).
- O link **Ajuda** – para abrir a Ajuda do Kaspersky Anti-Virus.
- O botão **Detectado** - para trabalhar com os arquivos de dados do aplicativo (veja página 84).
- O botão **Relatórios** – para abrir os relatórios dos componentes do aplicativo (ver página 85).
- O link **Suporte** – para abrir a janela com informações do sistema e links para os recursos de informações da Kaspersky Lab (veja página 30) (site do serviço de Suporte técnico, fórum).

NOTIFICAÇÕES

Se determinados eventos ocorrerem durante a operação do Kaspersky Anti-Virus, notificações especiais serão exibidas na tela em forma de mensagens pop-up, acima do ícone do aplicativo na barra de tarefas do Microsoft Windows.

Dependendo do grau de importância do evento para a segurança do computador, você poderá receber os seguintes tipos de notificações:

- **Alarme**. Ocorreu um evento de importância crítica, como a detecção de um vírus. Decida imediatamente como lidar com a ameaça. Este tipo de notificação está codificada pela cor vermelha.

- **Aviso**. Ocorreu um evento potencialmente perigoso, como a detecção de um objeto possivelmente perigoso. Você deverá decidir o nível de perigo que este evento representa. Este tipo de notificação está codificada pela cor amarela.

- **Informações**. Esta notificação fornece informações sobre eventos não-críticos. As notificações menores estão codificadas pela cor verde.

CONSULTE TAMBÉM:

Tipos de notificações..99

JANELA DE CONFIGURAÇÃO DO APLICATIVO

Você pode abrir a janela de configuração do Kaspersky Anti-Virus a partir da janela principal. Para tanto, clique no botão **Configurações** na parte superior da janela principal.

A janela de configuração está desenhada como a janela principal:

- a parte esquerda da janela oferece acesso rápido e fácil às configurações para o Antivírus de arquivos, tarefas de verificação de vírus, de atualização e opções de programa;

- a parte direita da janela contém uma lista de configurações para o componente Antivírus de arquivos, uma tarefa etc. selecionada na parte esquerda da janela.

CONSULTE TAMBÉM:

Configuração das configurações do aplicativo 70

ANTIVÍRUS DE ARQUIVOS

Antivírus de arquivos evita a infecção do sistema de arquivos do computador. Ele é carregado ao iniciar o sistema operacional, sendo executado na RAM do computador, verificando todos os arquivos abertos, salvos ou executados.

Por padrão, o Antivírus de arquivos verifica apenas arquivos novos ou modificados. O conjunto de configurações chamado de nível de segurança determina a forma de verificar os arquivos. Se o Antivírus de arquivos detectar uma ameaça, ele executará a ação predefinida.

O nível de proteção dos arquivos e da memória do computador é determinado pelas seguintes combinações de configurações:

- Configurações do escopo de proteção;
- Configurações que determinam o método de verificação utilizado;
- Configurações que determinam a verificação dos arquivos compostos (incluída a verificação de arquivos compostos grandes);
- Configurações que determinam o modo de verificação;
- Configurações usadas para pausar a operação do componente (por programação, durante a operação dos aplicativos selecionados).

Para modificar as configurações do Antivírus de arquivos:

1. Abra a janela principal do aplicativo e clique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, altere as configurações do componente que sejam necessárias.

NESTA SEÇÃO

ALGORITMO DE OPERAÇÃO DO COMPONENTE

O componente *Antivírus de arquivos* é carregado quando você inicializar o sistema operacional e é executado na memória do computador, verificando todos os arquivos abertos, salvos ou executados.

Por padrão, o componente Antivírus de arquivos verifica somente arquivos novos ou modificados; ou seja, os arquivos que foram adicionados ou alterados desde a verificação anterior. Os arquivos são verificados de acordo com o seguinte algoritmo:

1. O componente intercepta todas as tentativas de acessar qualquer arquivo feitas pelo usuário ou por qualquer programa.

2. O Antivírus de arquivos verifica nos bancos de dados do iChecker e do iSwift as informações sobre o arquivo interceptado e determina se o arquivo deve ser verificado, de acordo com as informações recuperadas.

A verificação consiste nas seguintes etapas:

- O arquivo é verificado quando à presença de vírus. Os objetos são detectados comparando-os com os bancos de dados dos aplicativos. O banco de dados contém descrições de todos os programas maliciosos e ameaças conhecidos no momento e os métodos para processá-los.

- Após a análise, você pode executar as seguintes ações com o Kaspersky Anti-Virus:

  a. Se for detectado um código malicioso no arquivo, o Antivírus de arquivos bloqueará o arquivo, criará uma cópia de *backup* e tentará executar a desinfecção. Depois de ser desinfetado com êxito o arquivo fica acessível ao usuário. Se a desinfecção falhar, o arquivo será excluído.

b. Se algum código possivelmente malicioso for detectado no arquivo (mas seu propósito malicioso não for confirmado), o arquivo passará pela desinfecção e será enviado para a área de armazenamento especial chamada *Quarentena*.

c. Se nenhum código malicioso for descoberto no arquivo, ele será restaurado imediatamente.

O aplicativo o notificará quando um arquivo infectado ou possivelmente infectado for detectado. Então, você deverá responder à notificação através do processamento da mensagem:

- colocar o objeto na Quarentena, permitindo que a nova ameaça seja verificada e processada posteriormente usando bancos de dados atualizados;
- excluir o objeto;
- Ignorar, se você tem certeza de que o objeto não pode ser malicioso.

CONSULTE TAMBÉM:

Antivírus de arquivos 37

ALTERANDO O NÍVEL DE SEGURANÇA

O nível de segurança é definido como uma configuração predefinida do componente Antivírus de arquivos. Os especialistas da Kaspersky Lab diferenciam três níveis de segurança. O usuário deve decidir o nível a ser selecionado de acordo com as condições de operação e a situação atual.

- Se o computador apresenta grande risco de estar infectado é necessário selecionar o nível de segurança alto.
- O nível recomendado fornece o equilíbrio ideal entre eficiência e segurança e é adequado na maioria dos casos.
- Ao trabalhar em um ambiente protegido (por exemplo, em uma rede corporativa com gerenciamento de segurança centralizado) ou com aplicativos que consomem recursos, é recomendável selecionar o nível de segurança baixo.

Antes de ativar o nível de segurança Baixo, é recomendável executar uma verificação completa do computador com o nível de segurança Alto.

Se nenhum dos níveis predefinidos atender às suas necessidades, você mesmo poderá definir as Configurações do Antivírus de arquivos. Como resultado, o nome do nível de segurança será alterado para **Personalizado**. Para restaurar as configurações padrão do componente, selecione um dos níveis de segurança predefinidos.

Para alterar o nível de segurança do componente Antivírus de arquivos, faça o seguinte:

1. Abra a janela principal do aplicativo e clique no botão **Configurações** na parte superior da janela.
2. Selecione o nível de segurança necessário na janela que será aberta.

ALTERANDO AS AÇÕES A SEREM EXECUTADAS COM OS OBJETOS DETECTADOS

Como resultado da verificação, o Antivírus de arquivos atribui um dos seguintes status aos objetos detectados:

- Status do programa malicioso (como *vírus*, *cavalo de Troia*);

- *possivelmente infectado*, quando a verificação não pode determinar se o objeto está infectado. Isso significa que o aplicativo detectou no arquivo uma sequência de código de um vírus desconhecido ou o código modificado de um vírus conhecido.

Se, ao verificar vírus em um arquivo, o Kaspersky Anti-Virus descobrir arquivos infectados ou possivelmente infectados, as ações subsequentes do Antivírus de arquivos dependerão do status dos objetos e da ação selecionada.

Por padrão, todos os arquivos infectados estão sujeitos a desinfecção e todos os arquivos potencialmente infectados estão sujeitos a quarentena.

Todas as ações possíveis são mostradas na tabela a seguir.

SE A AÇÃO SELECIONADA FOR	QUANDO UM OBJETO PERIGOSO FOR DETECTADO
☑ **Desinfetar** ☐ **Excluir se a desinfecção falhar**	O acesso ao objeto é bloqueado, e é feita uma tentativa de desinfetá-lo. Uma cópia do objeto é armazenada no Backup. Se ele for desinfetado com êxito, será retornado ao usuário para ser usado normalmente. Se o objeto não puder ser tratado, será movido a Quarentena. As informações relevantes são registradas no relatório. Posteriormente, você pode tentar desinfetar esse objeto.
☑ **Desinfetar** ☑ **Excluir se a desinfecção falhar**	O acesso ao objeto é bloqueado, e é feita uma tentativa de desinfetá-lo. Uma cópia do objeto é armazenada no Backup. Se ele for desinfetado com êxito, será retornado ao usuário para ser usado normalmente. Se o objeto não puder ser desinfetado, ele será excluído.
☐ **Desinfetar** ☑ **Excluir**	O Antivírus de arquivos bloqueará o acesso ao objeto e o excluirá.
☑ **Bloquear usuário infectante por... horas**	Bloqueia a conexão do usuário atual com o servidor, se forem feitas tentativas de copiar um objeto infectado ou possivelmente infectado. Essa ação pode ser aplicada adicionalmente às ações relacionadas ao processamento do arquivo (desinfecção ou exclusão). Se o usuário sair de uma sessão e entrar no sistema novamente, o Kaspersky Anti-Virus considerará uma conexão diferente, e a proibição será suspensa.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup do objeto e a armazena no Backup para permitir a restauração ou desinfecção posterior.

Com o status *potencialmente infectado*, o objeto é movido a Quarentena sem uma tentativa de desinfecção.

➡ *Para alterar a ação específica a ser executada nos objetos detectados faça o seguinte:*

1. Abra a janela principal do aplicativo e clique no botão botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na seção **Ação**, selecione a ação requerida.

CRIANDO UM ESCOPO DE PROTEÇÃO

O escopo de proteção compreende o local dos objetos a serem verificados e também o tipo de arquivos a serem verificados. Por padrão, o Kaspersky Anti-Virus verifica apenas os arquivos que podem estar infectados, abertos em qualquer disco rígido, unidade de rede ou mídia removível.

Você pode ampliar ou restringir o escopo de proteção adicionando / removendo objetos a serem verificados, ou alterando os tipos de arquivos a serem verificados. Por exemplo, você quer verificar apenas os arquivos .exe executados

em unidades de rede. Entretanto, certifique-se de que seu computador não ficará exposto ao risco de infecção ao reduzir o escopo de proteção.

Ao selecionar os tipos de arquivos, lembre-se do seguinte:

- Há uma série de formatos de arquivos que possuem risco bastante baixo de ter códigos maliciosos infiltrados neles e posteriormente ativados ((por exemplo, *.txt*). Contrariamente, há formatos que contêm ou podem conter códigos executáveis, como por exemplo *.exe*, *.dll*, *.doc*. O risco de ativar o código malicioso nesses arquivos é bastante alto.

- Lembre-se de que um invasor pode enviar um vírus para seu computador com a extensão *.txt* que, na verdade, é um arquivo executável renomeado como um arquivo *.txt*. Se você selecionou a opção **Arquivos verificados por extensão**, esse arquivo será ignorado pela verificação. Se a configuração **Arquivos verificados por formato** foi selecionada, então, independentemente da extensão, o Antivírus de arquivos analisará o cabeçalho do arquivo, independentemente da sua extensão, descobrirá que se trata de um arquivo *.exe* e verificará se há a presença de vírus.

Ao especificar os tipos de arquivos que serão verificados, você estabelece que formatos de arquivo, tamanhos ou unidades serão verificados para detectar vírus quando forem abertos, executados ou salvos.

Para facilitar a configuração, todos os arquivos são divididos em dois grupos: *simples* e *compostos*. Os arquivos simples não contêm nenhum objeto (por exemplo, arquivos do tipo .txt). Os arquivos compostos incluem vários objetos e cada um deles também pode conter vários níveis aninhados. Estes objetos podem ser arquivos comprimidos, arquivos que contêm macros, planilhas, emails com anexos, etc.

Lembre-se que o Antivírus de arquivos apenas verificará os arquivos incluídos no escopo de proteção criado. Os arquivos não incluídos nesse escopo estarão disponíveis para serem utilizados sem prévia verificação. Isso aumenta o risco de infecção do seu computador!

➡ *Para editar a lista de verificação de objetos:*

1. Abraa janela principal do aplicativo e clique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Geral**, na seção **Escopo de proteção**, clique no link **Adicionar**.
4. Na janela **Selecionar objeto para verificar**, selecione um objeto e clique no botão **Adicionar**. Clique no botão **OK** após de adicionar todos os objetos desejados.
5. Para excluir um objeto da lista de objetos a serem verificados, desmarque as caixas ao lado dele.

➡ *Para alterar os tipos de objetos verificados:*

1. Abra a janela principal do aplicativo e clique no botão botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Geral**, na seção **Tipos de arquivos**, selecione as configurações desejadas.

USANDO A ANÁLISE HEURÍSTICA

Os objetos são verificados usando os bancos de dados que contêm descrições de todos os malwares conhecidos e os métodos de desinfecção correspondentes. O Kaspersky Anti-Virus compara cada objeto verificado com os registros do banco de dados para determinar com certeza se o objeto é malicioso e, em caso positivo, qual a sua classe de malware. Essa abordagem é chamada de *análise de assinaturas* e, por padrão, é usada sempre.

Como aparecem novos objetos maliciosos diariamente, sempre existem alguns malwares que não estão descritos nos bancos de dados e que podem ser detectados somente usando a análise heurística. Esse método inclui a análise das ações que um objeto executa no sistema. Se suas ações forem típicas de objetos maliciosos, provavelmente o objeto

será classificado como malicioso ou suspeito. Assim, novas ameaças podem ser detectadas mesmo antes de serem pesquisadas pelos analistas de vírus.

Além disso, você pode definir o nível de detalhamento das verificações. Esse nível define o equilíbrio entre a profundidade das buscas por novas ameaças, a carga sobre os recursos do sistema operacional e o tempo necessário para a verificação. Quando mais alto o nível de detalhamento, mais recursos e mais tempo serão necessários para a verificação.

➡ *Para usar a análise heurística e definir o nível de detalhamento das verificações:*

1. Abra a janela principal do aplicativo e clique no botão botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Desempenho** na seção **Métodos de Verificação**, verifique a caixa ☑ **Análise Heurística** e especifique o nível de detalhes para a verificação.

OTIMIZAÇÃO DA VERIFICAÇÃO

Para reduzir a duração das verificações e aumentar a velocidade de operação do Kaspersky Anti-Virus, você pode optar pela verificação apenas dos arquivos novos e os arquivos modificados desde a última análise. Esse modo se aplica a arquivos simples e compostos.

➡ *Para verificar apenas os arquivos novos e os arquivos que foram alterados desde a última verificação:*

1. Abra a janela principalclique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Desempenho**, marque a caixa ☑ **Verificar apenas os arquivos novos e alterados**.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS

Um método comum para ocultar vírus é o de incorporá-los aos arquivos compostos, como arquivos comprimidos, bancos de dados etc. Para detectar vírus que estão ocultos dessa forma, um arquivo composto deve ser descomprimido, o que pode reduzir significativamente a velocidade da verificação.

Os arquivos e pacotes de instalação que contêm objetos OLE são executados ao serem abertos, o que os torna mais perigosos que os arquivos comprimidos. Ao desativar a verificação de arquivos comprimidos e ativar a verificação de arquivos desse tipo, você protege seu computador contra a execução de código malicioso e, ao mesmo tempo, aumenta a velocidade de verificação.

Se um arquivo com um objeto OLE incorporado é um arquivo comprimido este será verificado durante a descompactação. Você pode ativar a verificação do arquivo comprimido para verificar arquivos com objetos OLE incorporados antes de sua descompactação. Porém, isso reduzirá consideravelmente a velocidade de verificação.

Por padrão, o Kaspersky Anti-Virus verifica apenas os objetos OLE incorporados.

➡ *Para modificar a lista de arquivos compostos verificados:*

1. Abra a janela principal do aplicativo e clique no botão botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Desempenho** na seção **Verificação de arquivos compostos**, marque as caixas dos tipos de arquivos compostos a serem verificados.

VERIFICANDO ARQUIVOS COMPOSTOS GRANDES

Ao verificar arquivos compostos grandes, sua descompactação preliminar pode levar muito tempo. É possível reduzir este tempo apenas se você executar a verificação do arquivo em segundo plano. Se for detectado um objeto malicioso enquanto você trabalha com esse arquivo, o aplicativo o notificará.

Para reduzir o tempo de acesso dos arquivos compostos, desative a descompactação de arquivos maiores que o tamanho especificado. Ao serem extraídos de um arquivo comprimido, os arquivos sempre serão verificados.

Se você deseja que o aplicativo descompacte arquivos grandes em segundo plano:

1. Abra a janela principal do aplicativo e clique no botão botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Desempenho**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.
4. Na janela **Arquivos compostos**, marque a caixa ☑ **Extrair arquivos compostos em segundo plano** e especifique o valor do tamanho mínimo de arquivo no campo abaixo.

Se você não deseja que o aplicativo descompacte arquivos grandes faça o seguinte:

1. Abra a janela principalclique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Desempenho**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.
4. Na janela **Arquivos compostos**, marque a caixa ☑ **Não descompactar arquivos compostos grandes** e especifique o valor do tamanho máximo do arquivo no campo abaixo.

ALTERANDO O MODO DE VERIFICAÇÃO

O Modo de verificação é a condição que aciona a atividade do Antivírus de arquivos. A configuração padrão do aplicativo é o modo inteligente, que determina se o objeto será verificado de acordo com as ações executadas nele. Por exemplo, ao trabalhar com um documento do Microsoft Office, o aplicativo verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação.

Você pode alterar o modo de verificação dos objetos. O modo de verificação deve ser selecionado de acordo com os arquivos com os quais você trabalha na maior parte do tempo.

Para alterar o modo de verificação dos objetos:

1. Abra a janela principal do aplicativo e clique no botão botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Adicional**, na seção **Modo de verificação**, selecione o modo desejado.

TECNOLOGIA DE VERIFICAÇÃO

Você também pode especificar as tecnologias que serão usadas pelo componente Antivírus de arquivos:

- **iChecker**. Essa tecnologia pode aumentar a velocidade de verificação, excluindo determinados objetos. Um objeto será excluído da verificação usando um algoritmo especial que leva em consideração a data de

lançamento dos bancos de dados do aplicativo, a data na qual o objeto foi verificado pela última vez, e quaisquer modificações às configurações da verificação.

Por exemplo, você tem um arquivo comprimido que foi verificado pelo aplicativo e ao qual foi atribuído o status *não infectado*. Na próxima verificação, o aplicativo vai ignorar esse arquivo comprimido, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Se a estrutura do arquivo comprimido tiver sido modificada porque um novo objeto foi adicionado, se as configurações de verificação tiverem sido alteradas ou se os bancos de dados do aplicativo tiverem sido atualizados, o aplicativo verificará o arquivo comprimido novamente.

A tecnologia iChecker tem algumas limitações: ela não é compatível com arquivos grandes e se aplica apenas aos objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

- **iSwift**. Essa tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam o sistema de arquivos NTFS. A tecnologia iSwift tem algumas limitações: ela é ligada ao local de um arquivo específico no sistema de arquivos e se aplica apenas a objetos em NTFS.

Para alterar a tecnologia de verificação de objetos:

1. Abraa janela principal do aplicativo e clique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Adicional**, na seção **Tecnologias de verificação**, selecione o valor de configuração desejado.

PAUSANDO O COMPONENTE: CRIANDO UMA PROGRAMAÇÃO

Quando programas que exigem muitos recursos do computador estão em execução, você pode pausar temporariamente a operação do componente Antivírus de arquivos para permitir um acesso mais rápido aos objetos. Para reduzir a carga e assegurar o acesso rápido a objetos, você pode programar a desativação do componente.

Para configurar uma programação para pausar o componente:

1. Abra a janela principalclique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Adicional**, na seção **Pausar tarefa**, marque a caixa ☑ **Em programação** e clique no botão **Programar**.
4. Na janela **Pausar tarefa**, especifique o período (no formato de 24 horas HH:MM) em que a proteção será pausada (campos **Pausar tarefas às** e **Reiniciar tarefa às**).

PAUSANDO O COMPONENTE: CRIANDO UMA LISTA DE APLICATIVOS

Quando programas que exigem muitos recursos do computador estão em execução, você pode pausar temporariamente a operação do componente Antivírus de arquivos para permitir um acesso mais rápido aos objetos. Para reduzir a carga e assegurar o acesso rápido a objetos, você pode configurar a desativação do componente ao trabalhar com determinados aplicativos.

Configurar a desativação do componente Antivírus de arquivos no caso de conflitos com determinados aplicativos é uma medida de emergência! Em caso de conflitos na operação do componente, comunique-se com o Serviço de suporte

técnico da Kaspersky Lab (http://usa.kaspersky.com/support/corporate/). Especialistas de suporte o ajudarão a solucionar operações simultâneas do Kaspersky Anti-Virus com os softwares de seu computador.

Para configurar a pausa do componente enquanto determinados aplicativos estão em uso:

1. Abra a janela principal do aplicativo e clique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e clique no botão **Personalizar**.
3. Na janela que será aberta, na aba **Adicional** na seção **Pausar tarefa** verifique o ☑ Na caixa **Ao iniciar o aplicativo** e clique no botão **Selecionar**.
4. Na janela **Aplicativos**, crie uma lista de aplicativos que pausarão o componente durante a execução.

RESTAURANDO AS CONFIGURAÇÕES DE PROTEÇÃO PADRÃO

Ao configurar o Antivírus de arquivos, você pode restaurar as configurações recomendadas a qualquer momento. Elas são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

Se você modificou a lista de objetos incluída na zona protegida ao configurar as configurações do Antivírus de arquivos, o aplicativo perguntará se deseja salvar essa lista para usá-la mais tarde ao restaurar as configurações iniciais.

Para restaurar as configurações de proteção padrão e para salvar a lista modificada de objetos incluídos na zona protegida:

1. Abra a janela principal do aplicativo e clique no botão **Configurações** na parte superior da janela.
2. Na janela que será aberta, selecione o componente **Antivírus de arquivos** e pressione o botão **Nível padrão**.
3. Na janela **Restaurar configurações** que será aberta, marque a caixa ☑ **Escopo de proteção**.

ESTATÍSTICAS DO ANTIVÍRUS DE ARQUIVOS

Todas as operações realizadas pelo Antivírus de arquivos são registradas em um relatório especial. Para ver a informação sobre a operação do componente, clique no link **Estatísticas**. Você verá um relatório detalhado sobre a operação do componente, agrupado em guias:

- Todos os objetos perigosos detectados durante o processo de proteção do sistema são enumerados na aba *Detectado*. Aqui você encontrará o caminho completo até a localização de cada objeto e o status atribuído a ele pelo Antivírus de arquivos: se for estabelecido com êxito qual programa malicioso infetou o objeto, será atribuído a ele o status apropriado. Por exemplo, vírus, cavalo de Troia etc. Se o tipo de impacto malicioso não puder ser definido com exatidão, será atribuído ao objeto o status *suspeito*. A ação aplicada ao objeto (detectado, não encontrado, desinfetado) também é exibida ao lado do status.

  Para que esta aba não contenha informações sobre os objetos desinfetados, desmarque a caixa ☑ **Mostrar objetos desinfetados**.

- A lista completa de eventos ocorridos durante o uso do Antivírus de arquivos é mantida na aba *Eventos*. Os eventos podem ser dos seguintes tipos:
  - *Informação* (por exemplo, objeto não processado, ignorado por tipo).
  - *Advertência* (por exemplo, um vírus é detectado).
  - *Comentário* (por exemplo, o arquivo comprimido está protegido por senha).

Como regra, as mensagens informativas são mensagens tipo referência e não são de interesse específico. Você pode desativar a visualização das mensagens informativas. Para fazê-lo, desmarque a caixa ☑ **Mostrar todos os eventos**.

- As *estatísticas* da verificação aparecem na aba apropriada. Aqui você encontrará o número total de objetos verificados e colunas especiais exibem separadamente quantos objetos do total verificado são arquivos comprimidos, quantos deles são perigosos, quantos foram desinfetados, quantos foram colocados em quarentena e etc.
- As configurações que o Antivírus de arquivos está executando são exibidas na guia *Configurações*. Use o link **Alterar configurações** para configurar rapidamente o componente.
- A guia *Usuários proibidos* exibe uma lista de usuários cujos computadores foram proibidos quando tentaram copiar um arquivo infectado ou possivelmente infectado no servidor.

TRATAMENTO DE OBJETO RETIDO

No Kaspersky Anti-Virus para Windows Servers, o acesso aos arquivos infectados é bloqueado se eles estiverem sendo desinfectados e se tiverem sido excluídos nos casos em que não puderam ser desinfectados ou excluídos.

Para obter novamente o acesso aos objetos bloqueados, você deve primeiramente tentar desinfetá-los. Se um objeto for desinfetado com êxito ele será restaurado para ser usado normalmente. Se o objeto não puder ser desinfetado, você terá a opção de *excluir* ou *ignorar* o objeto. Neste último caso o acesso ao arquivo será restaurado. Porém, isso aumenta consideravelmente o risco de infecção no servidor. É altamente recomendável não ignorar objetos maliciosos.

➡ *Para obter acesso aos objetos bloqueados para desinfetá-los faça o seguinte:*

1. Abra a janela principal do aplicativo e clique no botão **Detectado**.
2. Na janela que será aberta, na aba **Ativar ameaças**, selecione os objetos necessários e clique no link **Neutralizar tudo**.

CONSULTE TAMBÉM:

Alterando as ações a serem executadas com os objetos detectados 39

VERIFICAÇÃO DE VÍRUS DO SERVIDOR

O Kaspersky Anti-Virus 6.0 para Windows Servers MP4 pode verificar itens separados (arquivos, pastas, discos, mídia removível) ou o computador todo para vírus. A verificação de vírus descarta a possibilidade de disseminação de código malicioso que, por algum motivo, não tenha sido detectado pelo Antivírus de arquivos.

Kaspersky Anti-Virus 6.0 para Windows Servers MP4 é composto das seguintes tarefas padrão para verificação de vírus:

Verificação

Verificação de objetos selecionados pelo usuário. Você pode verificar qualquer objeto do sistema de arquivos do computador.

Verificação completa

Uma verificação completa de todo o sistema. Os seguintes objetos são verificados por padrão: memória do sistema, programas carregados na inicialização, backup do sistema, bancos de dados de email, discos rígidos, mídias de armazenamento removíveis e unidades de rede.

Verificação rápida

Verificação de vírus nos objetos de inicialização do sistema operacional.

Por padrão, essas tarefas operam com as configurações recomendadas. Estas configurações podem ser modificadas e as tarefas podem ser agendadas para serem operadas.

Além disso, você pode verificar vírus em qualquer objeto sem criar uma tarefa de verificação especial. Um objeto a ser verificado pode ser selecionado usando-se a interface do Kaspersky Anti-Virus ou ferramentas padrão do Microsoft Windows Servers (por exemplo, **Windows Explorer** ou **Desktop** etc.). Coloque o cursor sobre o nome do objeto desejado, clique com o botão direito do mouse para abrir o menu de contexto do Microsoft Windows e selecione a opção **Verificar vírus**.
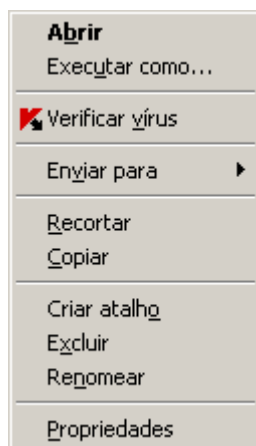
Figura 7. Menu de contexto do Microsoft Windows

Adicionalmente, seguindo uma verificação, você pode visualizar o relatório do verificador, que contém informações completas sobre os eventos que ocorreram durante a execução de tarefas.

Para mudar a configuração de qualquer tarefa de verificação de vírus, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.

4. Na janela que se abrirá, faça as mudanças requeridas na configuração da tarefa que você selecionou.

Para alternar para o relatório da verificação de vírus, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Clique no botão **Relatórios**.

NESTA SEÇÃO

INICIANDO A VERIFICAÇÃO DE VÍRUS

Você pode iniciar uma verificação de vírus usando uma das duas seguintes maneiras:

- a partir do menu de contexto do Kaspersky Anti-Virus;
- a partir da janela principal do Kaspersky Anti-Virus.

A informação sobre a execução da tarefa será exibida na janela principal do Kaspersky Anti-Virus.

Além disso, você pode selecionar um objeto para ser verificado com as ferramentas padrão do sistema operacional Microsoft Windows (por exemplo, na janela do programa **Explorer** ou na sua **Área de trabalho**, etc.).
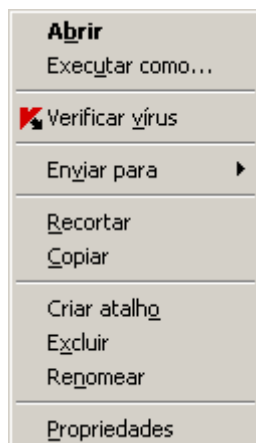
Figura 8. Menu de contexto do Microsoft Windows

Para começar uma tarefa de verificação de vírus a partir do menu de contexto, faça o seguinte:

1. Clique com o botão direito do mouse no ícone do aplicativo na área de notificação da barra de tarefas.

2. Selecione o item **Verificação** a partir do menu suspenso. Na janela principal do aplicativo que irá se abrir, selecione a tarefa de **Verificação** (**Verificação completa**, **Verificação rápida**) requerida. Se necessário, configure a tarefa selecionada e clique no botão **Iniciar verificação**.

3. Alternativamente, você pode selecionar o item **Verificação completa** a partir do menu de contexto. Isso iniciará uma verificação completa do computador. As informações sobre o progresso da tarefa serão exibidas na janela principal do Kaspersky Anti-Virus.

Para iniciar a tarefa de verificação de vírus a partir da janela principal do aplicativo:

1. Abra a janela principal do aplicativo.

2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).

3. Clique no botão **Iniciar verificação** para a seleção selecionada. O andamento da tarefa será exibido na janela principal do aplicativo.

Para iniciar uma tarefa de verificação de vírus para um objeto selecionado a partir do menu de contexto do Microsoft Windows:

1. Clique com o botão direito do mouse no nome do objeto selecionado.

2. Selecione o item **Verificar vírus** no menu de contexto que se abre. O progresso e os resultados da execução da tarefa serão exibidos na janela de estatísticas.

CRIANDO UMA LISTA DE OBJETOS A SEREM VERIFICADOS

Cada tarefa de verificação de vírus possui sua própria lista de objetos padrão. Para visualizar uma lista de objetos, selecione o nome da tarefa (tal como **Verificação completa**) na seção **Verificar** da janela principal do aplicativo. A lista de objetos será mostrada na parte direita da janela.

As listas de objetos a verificar já são geradas para tarefas padrão criadas na instalação do aplicativo.

Para a conveniência do usuário, você pode adicionar categorias para a abrangência do verificador, tais como caixas de correio do usuário, RAM, objetos inicializadores, backup do sistema operacional, e arquivos na pasta do Quarentena do Kaspersky Anti-Virus .

Alem disso, quando você adiciona uma pasta que contém objetos embutidos na abrangência do verificador, você pode editar a recursão. Para tanto, selecione o objeto requerido a partir da lista de objetos para verificar, abra o menu de contextos, e use a opção **Incluir subpastas**.

➧ *Para criar uma lista de objetos para verificar, faça o seguinte:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Clique no link **Adicionar** para a seção selecionada.
4. Na janela **Selecionar objeto para verificar** que irá se abrir, selecione um objeto e clique no botão **Adicionar**. Clique no botão **OK** após de adicionar todos os objetos desejados. Para excluir quaisquer objetos da lista de objetos para verificar, desmarque as caixas próximas a ele. Para remover um objeto da lista, selecione-o e clique no link **Excluir**.

ALTERANDO O NÍVEL DE SEGURANÇA

O nível de segurança é um conjunto predefinido de configurações de verificação. Os especialistas da Kaspersky Lab diferenciam três níveis de segurança. Você deve decidir qual nível selecionar, baseado nas suas próprias preferências:

- Se você suspeitar que seu computador possui altas chances de se tornar infectado, selecione Alto nível de segurança.
- O nível recomendado é adequado na maioria dos casos, e é recomendado para o uso por especialistas do Kaspersky Lab.
- Se você usar aplicativos que exigem recursos de RAM consideráveis, selecione o nível de segurança Baixo, pois nesse modo o aplicativo exige menos recursos do sistema.

Se nenhum dos níveis predefinidos atender às suas necessidades, você poderá configurar a verificação como quiser. Como resultado, o nome do nível de segurança será alterado para **Personalizado**. Para restaurar as configurações de verificação padrão, selecione um dos níveis de segurança predefinidos. Por padrão, a verificação é definida no nível **Recomendado**.

➧ *Para alterar o nível de segurança definido, execute as seguintes ações:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que se abre, na seção **Nível de segurança**, ajuste o deslizador na balança. Ao ajustar o nível de segurança, você define a taxa da velocidade do verificador e o número total de arquivos verificados: quanto menos arquivos estiverem sujeitos a análise para vírus, maior será a velocidade de verificação. Você também pode clicar no botão **Personalizar** e modificar as configurações requeridas na janela que se abre. O nível de segurança irá mudar para **Personalizado**.

ALTERANDO AS AÇÕES A SEREM EXECUTADAS COM OS OBJETOS DETECTADOS

Se um verificador de vírus identifica um objeto como infectado ou suspeito, o processamento subsequente pelo aplicativo vai depender do status do objeto e da ação selecionada.

Baseado nos resultados da verificação, um objeto pode receber um dos seguintes status:

- Status do programa malicioso (como *vírus*, *cavalo de Troia*);
- *Possivelmente infectado*, quando a verificação não pode determinar se o objeto está infectado. Isso acontece quando o aplicativo detecta no arquivo uma sequência de código de um vírus desconhecido ou de código de um vírus conhecido modificado.

Por padrão, todos os arquivos infectados estão sujeitos à desinfecção e todos os arquivos possivelmente infectados são colocados na Quarentena.

SE A AÇÃO SELECIONADA FOR	QUANDO UM OBJETO MALICIOSO/POSSIVELMENTE INFECTADO FOR DETECTADO
Perguntar o que fazer ao concluir a verificação	O aplicativo adiará o processamento de objetos até a conclusão da verificação. Quando a verificação estiver completa, o programa pedirá ao usuário ações para cada um dos arquivos uma após a outra.
Perguntar o que fazer durante a verificação	O Antivírus de arquivos exibirá uma mensagem de aviso com informações sobre o programa maliciosos que infectou ou possivelmente infectou o arquivo, fornecendo opções de ação.
Não perguntar o que fazer	O aplicativo criará um relatório com informações sobre os objetos detectados, sem processá-los ou notificar o usuário. Esse modo do aplicativo não é recomendável, pois ele deixa objetos infectados ou possivelmente infectados no computador, tornando a infecção praticamente inevitável.
Não perguntar o que fazer ☑ **Desinfetar**	O aplicativo criará um relatório com informações sobre os objetos detectados, sem processá-los ou notificar o usuário. Esse modo do aplicativo não é recomendável, pois ele deixa objetos infectados ou possivelmente infectados no computador, tornando a infecção praticamente inevitável.
Não perguntar o que fazer ☑ **Desinfetar** ☑ **Excluir se a desinfecção falhar**	O aplicativo tentará desinfetar o objeto sem solicitar a confirmação do usuário. Se o objeto não puder ser desinfetado, ele será excluído. Uma cópia é salva no Backup.
Não perguntar o que fazer ☐ **Desinfetar** ☑ **Excluir**	O aplicativo exclui o objeto automaticamente.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup do objeto e a armazena no Backup para permitir a restauração ou desinfecção posterior.

Com o status *potencialmente infectado*, o objeto é movido a Quarentena sem uma tentativa de desinfecção.

➧ *Para alterar a ação específica a ser executada nos objetos detectados faça o seguinte:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na seção **Ação**, digite as alterações necessárias na janela que irá se abrir.

ALTERANDO O TIPO DE OBJETOS A SEREM VERIFICADOS

Ao especificar o tipo de objetos a serem verificados, você estabelece quais formatos e tamanhos de arquivos irão ser verificados quanto a vírus quando a verificação de vírus selecionada for executada.

Ao selecionar os tipos de arquivos, lembre-se do seguinte:

- Certos formatos de arquivos (tais como *.txt*) possuem um risco um tanto baixo de possuírem códigos maliciosos infiltrados neles e subsequentemente ativados neles. Ao mesmo tempo, há formatos que contêm ou que podem conter um código executável (como *exe*, *dll*, *doc*). O risco de infiltração e ativação de código malicioso nesses arquivos é bastante grande.

- Lembre-se de que um invasor pode enviar um vírus para seu computador com a extensão *.txt* que, na verdade, é um arquivo executável renomeado como um arquivo *.txt*. Se você selecionou a opção **Arquivos verificados por extensão**, tal arquivo será pulado pelo verificador. Se a opção **Arquivos verificados por formato** for selecionada, independentemente da extensão, a proteção de arquivos analisará o título do arquivo e pode determinar que o arquivo é um arquivo .exe. Esse arquivo seria verificado cuidadosamente quanto à presença de vírus.

Para alterar os tipos de objetos verificados:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .
5. Na janela que irá se abrir, na aba **Escopo**, na seção **Tipos de arquivos**, selecione a configuração requerida.

OTIMIZAÇÃO DA VERIFICAÇÃO

Você pode diminuir o tempo de verificação e apressar o Kaspersky Anti-Virus. Isso é possível verificando apenas os arquivos novos e aqueles que foram alterados desde a última vez que foram verificados. Esse modo se aplica a arquivos simples e compostos.

Adicionalmente, você pode impor uma restrição à duração da verificação. Ao término do período especificado, a verificação dos arquivos será interrompida. Você também pode limitar o tamanho do arquivo sendo verificado. O arquivo será pulado se o tamanho exceder o valor que você determinou.

Para verificar somente arquivos novos e modificados, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .
5. Na janela que será aberta, na aba **Escopo**, na seção **Otimização da verificação**, marque a caixa **Verificar somente arquivos novos e alterados**.

Para impor uma restrição de tempo para a duração da verificação:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .

5. Na janela que será aberta, na aba **Escopo**, na seção **Otimização da verificação**, marque a caixa ☑ **Interromper a verificação se levar mais de** que e especifique a duração da verificação no campo próximo a ela.

➡ *Para limitar o tamanho do arquivo a ser verificado, faça o seguinte:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .
5. Na janela que irá se abrir, na aba **Escopo**, clique no botão **Adicional**.
6. Na janela **Arquivos compostos** que irá se abrir, marque a caixa ☑ **Não descompacte arquivos compostos grandes** e especifique o tamanho do arquivo no campo próximo a ela.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS

Um método comum de esconder vírus é embutindo-o em arquivos compostos: arquivos, bancos de dados etc. Para detectar os vírus que estão escondidos desta forma, um arquivo composto deve ser descomprimido, o que pode reduzir a velocidade da verificação significativamente.

Para cada tipo de arquivo composto, você pode selecionar a verificação de todos os arquivos ou apenas dos arquivos novos. Para fazê-lo, use o link ao lado do nome do objeto. Ele muda seu valor quando você clica nele. Se você selecionar o modo de verificação Verificar apenas os arquivos novos e alterados, você não conseguirá selecionar quais tipos de arquivos compostos serão verificados.

➡ *Para modificar a lista de arquivos compostos verificados:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .
5. Na janela que irá se abrir, na aba **Escopo**, na seção **Verificação de arquivos compostos**, selecione o tipo requerido de arquivos compostos a ser verificado.

ALTERANDO O MÉTODO DE VERIFICAÇÃO

Você pode usar a *análise heurística* como método de verificação. Ela analisa as ações que um objeto executa no sistema. Se suas ações forem típicas de objetos maliciosos, provavelmente o objeto será classificado como malicioso ou suspeito.

Adicionalmente, você pode configurar o nível de detalhe para a análise heurística movendo a barra deslizadora para uma das seguintes posições: **superficial**, **médio**, ou **profunda**.

Além deste método, você pode usar a Verificação Rootkit. *O Rootkit* é um conjunto de ferramentas que pode esconder aplicativos maliciosos em seu sistema operacional. Esses utilitários são introduzidos no sistema e ocultam sua presença e a presença de processos, pastas e chaves do Registro de outros programas maliciosos instalados com o rootkit. Se a verificação estiver ativada, você pode especificar o nível detalhado (análise avançada) para detectar rootkits. Esses programas serão verificados cuidadosamente através da análise de um grande número de objetos diversos.

Para especificar o método de verificação a ser usado:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .
5. Na janela que irá se abrir, na aba **Adicional**, na seção **Métodos de verificação**, selecione as tecnologias de verificação requeridas.

TECNOLOGIA DE VERIFICAÇÃO

Adicionalmente, você pode especificar a tecnologia que será usada durante a verificação:

- **iChecker**. Essa tecnologia pode aumentar a velocidade de verificação, excluindo determinados objetos. Um objeto será excluído da verificação usando um algoritmo especial que leva em consideração a data de lançamento dos bancos de dados do aplicativo, a data na qual o objeto foi verificado pela última vez, e quaisquer modificações às configurações da verificação.

  Por exemplo, você tem um arquivo dentro de arquivo comprimido que foi verificado pelo Kaspersky Anti-Virus e recebeu o status de *não-infectado*. Na próxima verificação, o aplicativo vai ignorar esse arquivo comprimido, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Se a estrutura do arquivo comprimido tiver sido modificada porque um novo objeto foi adicionado, se as configurações de verificação tiverem sido alteradas ou se os bancos de dados do aplicativo tiverem sido atualizados, o aplicativo verificará o arquivo comprimido novamente.

  Existem limitações ao iChecker: ele não funciona com arquivos grandes e somente se aplica aos objetos com uma estrutura que o aplicativo reconhece (por exemplo, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

- **iSwift**. Essa tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam o sistema de arquivos NTFS. A tecnologia iSwift tem algumas limitações: ela é ligada ao local de um arquivo específico no sistema de arquivos e se aplica apenas a objetos no NTFS.

Para usar a tecnologia de verificação de objetos, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .
5. Na janela que irá se abrir, na aba **Adicional**, na seção **Tecnologias de verificação**, ative a tecnologia requerida.

EFICIÊNCIA DO COMPUTADOR DURANTE A EXECUÇÃO DE TAREFAS

As tarefas de verificação de vírus podem ser adiadas a fim de limitar a carga da CPU e dos subsistemas de armazenamento em disco.

A execução de tarefas de verificação aumenta a carga da CPU e dos subsistemas de disco, tornando os outros aplicativos mais lentos. Por padrão, se tal situação ocorrer, o Kaspersky Anti-Virus irá pausar as tarefas de verificação de vírus e lançar recursos do sistema para os aplicativos do usuário.

Entretanto, vários aplicativos serão iniciados imediatamente quando os recursos da CPU estiverem disponíveis, sendo executados em segundo plano. Para que a verificação não dependa do desempenho desses aplicativos, os recursos do sistema não devem ser disponibilizados para eles.

Note que esta configuração pode ser ajustada individualmente para cada tarefa de verificação de vírus. Nesse caso, a configuração de uma tarefa específica terá prioridade maior.

Para adiar a execução das tarefas de verificação se este reduzir a atividade de outros aplicativos, faça o seguinte:

1. Abra a janela principaldo aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .
5. Na janela que será aberta, na aba **Adicional**, na seção **Métodos de verificação**, marque a caixa **Conceder recursos a outros aplicativos**.

PAUSANDO A TAREFA: CRIANDO A PROGRAMAÇÃO

Quando programas que exigem muitos recursos do computador estão em execução, você pode pausar temporariamente a operação do componente Antivírus de arquivos. Para reduzir a carga e assegurar o acesso rápido a objetos, você pode programar a desativação do componente.

Para configurar a programação para pausar a tarefa:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Selecione o item **Personalizar** a partir do menu suspenso.
5. Na janela que será aberta, na guia **Adicional**, na seção **Pausar tarefa**, marque a caixa **Em programação** e clique no botão **Programar**.
6. Na janela **Pausar tarefa**a, especifique o período (no formato de 24 horas HH:MM) em que a proteção será pausada (campos **Pausar tarefas às** e **Reiniciar tarefa às**).

PAUSANDO O COMPONENTE: CRIANDO UMA LISTA DE APLICATIVOS

Quando programas que exigem muitos recursos do computador estão em execução, você pode pausar temporariamente a operação do componente Antivírus de arquivos. Para reduzir a carga e assegurar o acesso rápido a objetos, você pode configurar uma lista de aplicativos específicos para a desativação do componente.

Para configurar a pausa do componente enquanto determinados aplicativos estão em uso:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Selecione o item **Personalizar** a partir do menu suspenso.

5. Na janela que será aberta, na aba **Adicional** na seção **Pausar tarefa** verifique o☑ Na caixa **Ao iniciar o aplicativo** e clique no botão **Selecionar**.

6. Na janela **Aplicativos**, crie uma lista de aplicativos que pausarão o componente durante a execução.

MODO DE EXECUÇÃO: ESPECIFICANDO UMA CONTA

Você pode especificar uma conta usada pelo aplicativo ao executar uma verificação de vírus.

➡ *Para iniciar a tarefa com os privilégios de uma conta de usuário diferente:*

1. Abra a janela principal do aplicativo.

2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).

3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.

4. Na janela que será aberta, na seção **Nível de segurança**, clique no botão **Personalizar** .

5. Na janela que será aberta, na aba **Modo de execução**, na seção **Usuário**, marque a caixa ☑ **Executar tarefa como**. Especifique o nome do usuário e a senha.

MODO DE OPERAÇÃO: CRIANDO UM AGENDAMENTO

Todas as tarefas de verificação de vírus podem ser iniciadas manualmente, ou por agendamento.

A configuração padrão para tarefas criadas quando o programa está instalado é desativado (Off). A exceção é a tarefa de verificação rápida, que é executada sempre que você inicia seu computador.

Ao criar uma agenda de inicialização de tarefas, é necessário configurar o intervalo das verificações.

Se não for possível iniciar a tarefa por qualquer motivo (por exemplo, o computador não estava ligado em um período especificado), você pode configurar a tarefa para começar automaticamente assim que for possível.

➡ *Para editar a programação de tarefas de verificação:*

1. Abra a janela principal do aplicativo.

2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).

3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.

4. Na janela que irá se abrir, pressione o botão **Alterar** na seção **Modo de execução**.

5. Faça as mudanças necessárias na janela **Programar** que irá se abrir.

➡ *Para configurar execuções automáticas de tarefas ignoradas:*

1. Abra a janela principal do aplicativo.

2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).

3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.

4. Na janela que irá se abrir, pressione o botão **Alterar** na seção **Modo de execução**.

5. Na janela **Programar** que irá se abrir, na seção **Configurações da programação**, marque a caixa ☑ **Executar tarefa se ignorada**.

CARACTERÍSTICAS DA INICIALIZAÇÃO DA TAREFA AGENDADA

Todas as tarefas de verificação de vírus podem ser iniciadas manualmente, ou por agendamento.

As tarefas agendadas apresentam uma funcionalidade adicional, por exemplo, você pode marcar a caixa *Pausar verificação programada quando a proteção de tela estiver inativa ou o computador desbloqueado*. Essa funcionalidade adia a execução da tarefa até que o usuário tenha concluído seu trabalho no computador. Assim, a tarefa de verificação não consumirá recursos do sistema durante o trabalho.

Para executar as tarefas de verificação somente quando o computador não estiver mais em uso:

1. Abra a janela principal do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Verificação completa** na seção **Verificação rápida**.
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que se abrirá, na seção **Modo de execução**, marque a caixa ☑ **Pausar a verificação programada quando a proteção de tela estiver inativa e o computador estiver desbloqueado**.

ESTATÍSTICAS DO VERIFICAÇÃO DE VÍRUS

As informações gerais sobre cada tarefa de verificação de vírus são exibidas na janela de estatísticas. Aqui você pode verificar quantos objetos foram verificados e quantos objetos perigosos e suspeitos, que estão sujeitos a processamento, foram detectados. Adicionalmente, aqui você pode achar informação sobre o tempo de início e término da execução da última tarefa e sobre a duração do verificação.

As informações gerais sobre resultados de verificação são agrupadas nas seguintes abas:

- A aba *Detectado* lista todos os objetos perigosos que foram detectados quando uma tarefa foi executada.
- A aba *Eventos* lista todos os eventos ocorridos durante a execução de uma tarefa.
- A aba *Estatísticas* fornece dados estatísticos sobre objetos verificados.
- A aba *Configurações* fornece as configurações que determinam a forma de execução de uma tarefa.

Se quaisquer erros ocorreram durante a verificação, tente executá-la novamente. Se a próxima tentativa voltar a apresentar erro, nós recomendamos que você salve o relatório sobre resultados da tarefa em um arquivo, usando o botão **Salvar como**. Então, contate o Serviço de Suporte Técnico, e envie o arquivo do relatório. Os especialistas do Kaspersky Lab certamente irão lhe ajudar.

Para ver as estatísticas de uma tarefa de verificação de vírus, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**), crie uma tarefa de verificação e inicialize-a. O progresso da tarefa será mostrado na janela principal. Clique no link **Detalhes** para alternar a janela de estatísticas.

DEFININDO CONFIGURAÇÕES DE VERIFICAÇÃO COMUNS PARA TODAS AS TAREFAS

Cada tarefa de verificação é executada de acordo com suas próprias configurações. Por padrão, as tarefas criadas na instalação do aplicativo são executadas com as configurações recomendadas por especialistas do Kaspersky Lab.

Você pode estabelecer configurações de verificação universais para todas as tarefas. Você irá usar um conjunto de propriedades usadas para verificar um objeto individual para vírus como o ponto de partida.

Para determinar configurações universais de verificação para todas as tarefas, faça o seguinte:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação**.
3. Na parte direita da janela, na seção **Outras configurações de tarefas**, clique no botão **Aplicar**. Confirme as configurações universais que você selecionou na caixa de diálogo que aparece.

RESTAURANDO AS CONFIGURAÇÕES DE VERIFICAÇÃO PADRÃO

Ao editar as configurações de tarefas, você sempre pode restaurar as configurações recomendadas. Elas são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

Para restaurar as configurações padrão de verificação de arquivos, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. Para a seção selecionada, clique no link com o nível de segurança pré-configurado.
4. Na janela que irá se abrir, pressione o botão **Nível padrão** na seção **Nível de segurança**.

ATUALIZANDO O APLICATIVO

Manter a proteção atualizada é um pré-requisito prévio de proteção confiável. Com o aparecimento diário de novos vírus, cavalos de Troia e softwares maliciosos, é importante atualizar periodicamente o aplicativo para manter seus dados pessoais sempre protegidos.

O componente de atualização do aplicativo descarrega e instala as seguintes atualizações no servidor:

- **Bancos de dados do aplicativo**

  A proteção de informação é garantida pelos bancos de dados do aplicativo. O Antivírus de arquivos os utiliza para pesquisar e desinfectar objetos perigosos no servidor. Os bancos de dados são adicionados por hora com registros de novas ameaças. Assim, é recomendável atualizá-los periodicamente.

- **Módulos do aplicativo**

  Além dos bancos de dados do aplicativo, você também pode atualizar os módulos deste. Os pacotes de atualização consertam as vulnerabilidades do aplicativo e adiciona ou melhora a funcionalidade existente.

Os servidores de atualização da Kaspersky Lab são as fontes principais das atualizações do Kaspersky Anti-Virus.

Para baixar as atualizações dos servidores com êxito, é necessário que seu computador esteja conectado à Internet. Por padrão, as configurações da conexão com a Internet são determinadas automaticamente. Se as configurações de proxy não forem corretamente configuradas automaticamente, as configurações da conexão podem ser ajustadas manualmente.

Durante uma atualização, os módulos e bancos de dados do aplicativo no seu computador são comparados com aqueles na fonte de atualização. Se o computador possuir a versão mais recente dos bancos de dados e dos módulos do aplicativo, aparecerá uma janela de notificação confirmando que a proteção do computador está atualizada. Se os bancos de dados e os módulos no computador e no servidor de atualização forem diferentes, o aplicativo baixará somente as partes necessárias das atualizações. Como nem todos os bancos de dados e módulos são baixados, a velocidade de cópia dos arquivos aumenta significativamente, economizando tráfego da Internet.

Antes de atualizar os bancos de dados, o Kaspersky Anti-Virus cria cópias de segurança dos bancos para que você possa usá-las novamente no futuro.

Você pode precisar da opção reversão se, por exemplo, os bancos de dados tornarem-se corrompidos durante o processo de atualização. Você pode reverter facilmente para a versão anterior e tentar atualizar os bancos de dados novamente.

Você pode copiar as atualizações recuperadas para uma fonte local enquanto faz a atualização do aplicativo. Este serviço permite a atualização de bancos de dados e módulos do aplicativo em computadores em rede para armazenar o tráfego da Internet.

Você também pode configurar a inicialização automática da atualização.

A seção **Atualizar** mostra o status atual dos bancos de dados do aplicativo.

Você pode visualizar o relatório das atualizações, que contém informações completas sobre eventos que ocorreram durante a atualização. Você também pode ter uma visão geral da atividade do vírus em www.kaspersky.com clicando no link **Revisão da atividade do vírus**.

➡ *Para editar as configurações de qualquer tarefa de atualização, faça o seguinte:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.

4. Na janela que se abrirá, faça as mudanças requeridas na configuração da tarefa que você selecionou.

Para alternar para atualizar relatório, faça o seguinte:

1. Abra a janela principal.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Clique no botão **Relatórios**.

NESTA SEÇÃO

COMEÇANDO A ATUALIZAÇÃO

Você pode iniciar a atualização do aplicativo a qualquer momento. As atualizações são baixadas de uma fonte de atualização selecionada.

Você pode atualizar o Kaspersky Anti-Virus usando um dos dois métodos suportados:

- Do menu de contexto.
- Da janela principal do aplicativo.

As informações sobre a atualização serão exibidas na janela principal do aplicativo.

Note que as atualizações são distribuídas para uma fonte local durante o processo de atualização, contanto que este serviço esteja ativado.

Para iniciar a atualização do Kaspersky Anti-Virus a partir do menu de contexto:

1. Clique com o botão direito do mouse no ícone do aplicativo na área de notificação da barra de tarefas.
2. Selecione o item **Atualização** no menu suspenso.

➧ *Para iniciar a atualização do Kaspersky Anti-Virus a partir da janela principal do aplicativo:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Clique no botão **Iniciar atualização**. O andamento da tarefa será exibido na janela principal do aplicativo.

RETORNANDO A ÚLTIMA ATUALIZAÇÃO

No começo do processo de atualização, o Kaspersky Anti-Virus cria uma cópia de segurança das bancos de dados atuais e módulos do aplicativo. Isso permite que o aplicativo continue trabalhando usando os bancos de dados anteriores, caso a atualização falhe.

A opção de reversão será útil se, por exemplo, parte dos bancos de dados for corrompida. As bancos de dados locais podem ser corrompidos pelo usuário ou por um programa malicioso, o que é possível somente se a auto-defesa do aplicativo estiver desativada. Você pode reverter facilmente para os bancos de dados anteriores e tentar atualizá-los posteriormente.

➧ *Para reverter para a versão anterior do banco de dados:*

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Clique no link **Reverter para os bancos de dados anteriores**.

SELECIONANDO UMA FONTE DE ATUALIZAÇÃO

A fonte de atualização é a fonte que contém as atualizações para os bancos de dados e módulos do aplicativo do Kaspersky Anti-Virus.

Você pode usar as seguintes fontes de atualização:

- *O Servidor administrador* é um repositório de atualizações centralizado, localizado no Kaspersky Administration Kit Servidor administrador (para mais detalhes, veja o Guia do Administrador para o Kaspersky Administration Kit).
- *Os servidores de atualização do Kaspersky Lab* são sites especiais que contêm atualizações para os bancos de dados e módulos do aplicativo para todos os produtos do Kaspersky Lab.
- *As pastas dos servidores FTP ou HTTP locais ou de rede* são servidores locais ou pastas que contêm as últimas atualizações.

Se você não tem acesso aos servidores de atualização da Kaspersky Lab (por exemplo, se o computador não estiver conectado à Internet), é possível ligar para o escritório principal da Kaspersky Lab no número +7 (495) 797-87-00 ou +7 (495) 645-79-39 e solicitar informações de contato dos parceiros da Kaspersky Lab que podem fornecer atualizações em disquetes ou discos comprimidos.

Você pode copiar as atualizações de um disco removível e transferi-las a um site FTP ou HTTP, ou armazená-las em uma pasta local ou de rede.

Ao solicitar as atualizações em mídia removível, especifique se você quer ter as atualizações para os módulos do aplicativo também.

Se um recurso externo à rede local for selecionado como fonte de atualização, é necessário ter uma conexão com a internet para a atualização.

Se forem selecionados vários recursos como fontes de atualização, o aplicativo tentará se conectar a cada um deles, começando pelo primeiro na lista, e recuperará as atualizações da primeira fonte disponível.

Para escolher uma fonte de atualização:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que irá se abrir, na seção **Atualizar configurações**, clique no botão **Configurar**.
5. Na janela que irá se abrir, na aba **Atualizar fonte**, clique no botão **Adicionar**.
6. Selecione um site FTP ou HTTP, ou digite seu endereço IP, nome simbólico ou URL na janela **Selecionar fonte de atualização** que irá se abrir.

CONFIGURAÇÕES REGIONAIS

Se você usar os servidores de atualização da Kaspersky Lab como fonte de atualização, poderá selecionar o local do servidor ideal para o download das atualizações. Os servidores da Kaspersky Lab estão localizados em diversos países. A escolha do servidor de atualização da Kaspersky Lab mais próximo economizará tempo e o download das atualizações será mais rápido.

Para escolher o servidor mais próximo:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que irá se abrir, na seção **Atualizar configurações**, clique no botão **Configurar**.
5. Na janela que irá se abrir, na aba **Fonte de atualização**, na seção **Configurações regionais**, selecione a opção **Selecionar da lista** e então selecione o país mais perto da sua localização atual na lista suspensa.

   Se você selecionar a opção **Autodetectar**, as informações sobre sua localidade serão copiadas dos registros do seu sistema operacional durante a atualização.

UTILIZANDO UM SERVIDOR DE PROXY

Se você estiver usando um servidor de proxy para conectar-se à Internet, você deverá ajustar suas configurações.

Para configurar o servidor proxy:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que irá se abrir, na seção **Atualizar configurações**, clique no botão **Configurar**.
5. Na janela que irá se abrir, edite as configurações do servidor de proxy na aba **Configurações de proxy**.

MODO DE EXECUÇÃO: ESPECIFICANDO UMA CONTA

O Kaspersky Anti-Virus possui uma característica que pode iniciar as atualizações de um programa a partir de um perfil diferente. Por padrão, esse serviço está desativado, e as tarefas são iniciadas usando a conta na qual você está registrado no sistema.

Uma vez que o aplicativo pode ser atualizado de uma fonte que você não possui acesso (tal como o diretório de atualizações de rede) ou direitos autorizados de usuário ao servidor proxy, você pode usar essa funcionalidade para executar atualizações do aplicativo usando o login de um usuário que possui tais privilégios.

Note que se você não executar a tarefa com privilégios, a atualização agendada será executada com os privilégios da conta do usuário atual. Se não houver usuários registrados atualmente no computador a execução de atualizações sob a conta de outro usuário não foi configurada e se as atualizações são executadas automaticamente, elas irão ser executadas com os privilégios do SISTEMA.

Para iniciar a tarefa com os privilégios de uma conta de usuário diferente:

1. Abra a janela principaldo aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que irá se abrir, na seção **Atualizar configurações**, clique no botão **Configurar**.
5. Na janela que irá se abrir, na aba **Adicional** , na seção **Modo de execução**, marque a caixa ☑ **Executar tarefa como**. Insira os dados de login que você deseja para iniciar a tarefa, conforme mostrado abaixo: nome de usuário e senha.

MODO DE OPERAÇÃO: CRIANDO UM AGENDAMENTO

Todas as tarefas de verificação de vírus podem ser iniciadas manualmente, ou por agendamento.

Ao criar uma agenda de inicialização de tarefas, é necessário configurar o intervalo das tarefas de atualização.

Se não for possível iniciar a tarefa por qualquer motivo (por exemplo, o computador não estava ligado em um período especificado), você pode configurar a tarefa para começar automaticamente assim que for possível.

Para editar a programação de tarefas de verificação:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que irá se abrir, pressione o botão **Alterar** na seção **Modo de execução**.
5. Faça as mudanças necessárias na janela **Programar** que irá se abrir.

Para configurar execuções automáticas de tarefas ignoradas:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.

4. Na janela que irá se abrir, pressione o botão **Alterar** na seção **Modo de execução**.

5. Na janela **Programar** que irá se abrir, na seção **Configurações da programação**, marque a caixa ☑ **Executar tarefa se ignorada**.

SELECIONANDO OBJETOS PARA ATUALIZAÇÃO

Os objetos para atualização são os componentes que serão atualizados:

- bancos de dados do aplicativo;
- módulos do aplicativo.

Os bancos de dados do aplicativo sempre são atualizados, mas os módulos do aplicativo serão atualizados somente se um modo apropriado estiver selecionado.

Se houver um conjunto de módulos do aplicativo na fonte de atualização durante atualização, o Kaspersky Anti-Virus irá baixar e instalar este quando o computador for reiniciado. As atualizações de módulos baixadas não serão instaladas até que o computador seja reiniciado.

Se a próxima atualização do aplicativo ocorrer antes do computador ser reiniciado, e por isso antes das atualizações do módulo do aplicativo previamente baixadas sejam instaladas, somente as assinaturas de ameaças serão atualizadas.

➧ *Se você quiser baixar e instalar atualizações para os módulos do aplicativo, faça o seguinte:*

1. Abra a janela principalprincipal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que irá se abrir, na seção **Atualizar configurações**, marque a caixa ☑ **Atualizar módulos de aplicativos**.

MUDANDO O MODO DE OPERAÇÃO DA ATUALIZAÇÃO DE TAREFAS

Você pode selecionar o modo de operação para a tarefa de atualização do Kaspersky Anti-Virus usando o assistente de configuração do aplicativo (ver seção "Configurar as configurações de atualização" na página 26). Você pode mudar o modo de operação selecionado.

A tarefa de atualização pode ser executada usando um dos seguintes modos:

- ◉ **Automaticamente**. O Kaspersky Anti-Virus verifica a fonte de atualização para pacotes de atualização em intervalos especificados. Se novas atualizações são encontradas, o Kaspersky Anti-Virus as descarrega e instala no computador. Este é o modo padrão.

  O Kaspersky Anti-Virus irá tentar fazer atualizações em intervalos especificados no pacote de atualizações anterior. Esta opção permite que o Kaspersky Lab regule a frequência de atualizações no caso de ataques de vírus e outras situações potencialmente perigosas. Seu aplicativo irá receber as últimas atualizações para os bancos de dados, ataques de rede e módulos de software em dia, excluindo assim a possibilidade de malware penetrar no seu computador.

- ◉ **Programado** (o intervalo de tempo varia dependendo da configuração). As atualizações serão executadas automaticamente de acordo com a programação criada.

- ◉ **Manualmente**. Ao selecionar esta opção, você mesmo executará as atualizações do aplicativo. O Kaspersky Anti-Virus irá lhe notificar quando as atualizações forem absolutamente necessárias.

Para configurar a programação de execução da tarefa de atualização:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que se abrirá, selecione o modo inicialização da tarefa de atualização na seção **Modo de execução**. Se a opção atualização programada for selecionada, criar o programação.

ATUALIZANDO DE UMA PASTA LOCAL

O procedimento para recuperar atualizações de uma pasta local é organizado da seguinte forma:

1. Um dos computadores na rede recupera o pacote de atualização do Kaspersky Anti-Virus do servidor da Kaspersky Lab ou de um servidor espelho que hospeda um conjunto atualizado de atualizações. As atualizações recuperadas são colocadas em uma pasta compartilhada.
2. Os outros computadores da rede acessam a pasta compartilhada para recuperar as atualizações.

O Kaspersky Anti-Virus 6.0 somente obtém pacotes de atualização dos servidores do Kaspersky Lab. É recomendável usar o Kaspersky Administration Kit para distribuir atualizações de outros aplicativos da Kaspersky Lab.

Para ativar o modo de distribuição de atualizações, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que será aberta, clique no botão **Personalizar**.
5. Na janela que se abre, na aba **Adicional**, na seção **Atualizar distribuição**, selecione a caixa ☑ **Copiar atualizações para pasta** e no campo abaixo especifique o caminho para uma pasta pública na qual as atualizações baixadas serão copiadas. Você também pode selecionar o caminho na janela que se abre ao clicar o botão **Procurar**.

Se você desejar que as atualizações do aplicativo sejam feitas da pasta compartilhada selecionada, faça o seguinte em todos os computadores da rede:

1. Abra a janela principal do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Para a seção selecionada, clique no link com o modo de execução pré-configurado.
4. Na janela que será aberta, clique no botão **Personalizar**.
5. Na janela que irá se abrir, na aba **Atualizar fonte**, clique no botão **Adicionar**.
6. Na janela **Selecionar atualização da fonte** que se abre, selecione uma pasta ou digite o caminho completo para ela no campo **Fonte**.
7. Desmarque a caixa ☑ **Atualização de servidores da Kaspersky Lab** na aba **Atualizar fonte**.

ESTATÍSTICAS DA ATUALIZAÇÃO

Você encontrará informações gerais sobre as tarefas de atualização na janela de estatísticas. Nessa janela, você também pode ver os eventos que ocorreram durante a execução de uma tarefa (na aba de *Eventos*) e ver a lista de configurações que determinam a execução da mesma (aba *Configurações*).

Se quaisquer erros ocorreram durante a verificação, tente executá-la novamente. Se a próxima tentativa voltar a apresentar erro, nós recomendamos que você salve o relatório sobre resultados da tarefa em um arquivo, usando o botão **Salvar como**. Então, contate o Serviço de Suporte Técnico, e envie o arquivo do relatório. Os especialistas do Kaspersky Lab certamente irão lhe ajudar.

Atualizações rápidas das estatísticas são exibidas na parte superior da janela Estatísticas. Ela inclui o tamanho das atualizações baixadas e instaladas, a velocidade e duração das atualizações e outras informações.

➧ *Para ver as estatísticas de uma tarefa de verificação de vírus, faça o seguinte:*

1. Abra a janela principal do aplicativo.

2. Na parte esquerda da janela, selecione a seção **Atualizar**, crie uma tarefa de atualização e a inicie. O progresso da tarefa será mostrado na janela principal. Você pode alternar a janela de estatísticas clicando no link **Detalhes**.

POSSÍVEIS PROBLEMAS DURANTE A ATUALIZAÇÃO

Quando você faz a atualização dos módulos do aplicativo do Kaspersky Anti-Virus ou assinaturas de ameaças, erros que estão associados com a configuração incorreta da atualização, problemas de conexão etc podem ocorrer. Esta seção Ajuda cobre a maior parte dos erros e dá dicas de como eliminá-los. Se você encontrar erros não abordados na seção Ajuda ou quiser recomendações detalhadas sobre como eliminá-los, tente achar a informação na Base de Conhecimento no portal da web de Suporte Técnico, na seção "If a program generated an error...". Se as recomendações dadas nesta seção não forem úteis para resolver o problema ou se não houver informações sobre o erro no Banco de Conhecimentos, envie um pedido para a Equipe de Suporte Técnico.

ERROS DE CONFIGURAÇÃO Os erros deste grupo ocorrem na maior parte devido a uma instalação incorreta do aplicativo, ou devido a modificações da configuração do mesmo, que resultaram em perda de funcionalidade. Recomendações gerais: Se os erros neste grupo forem gerados, nós recomendamos o reinício das atualizações. Se o erro persistir, contate o Suporte Técnico. Se o problema estiver conectado com uma incorreta instalação do aplicativo, recomendamos a reinstalação do mesmo.
Nenhuma fonte de atualização foi especificada Nenhuma das fontes contém arquivos de atualização. É possível que nenhuma fonte de atualização esteja especificada na configuração de atualização. Certifique-se de que a configuração das atualizações esteja configurada corretamente e tente novamente.
Erro na verificação da licença Este erro é gerado se a chave da licença usada pelo aplicativo estiver bloqueada e colocada na lista negra da licença.
Erro na obtenção de configurações da atualização Erro interno na obtenção das configurações da tarefa da atualização. Certifique-se de que a configuração das atualizações esteja configurada corretamente e tente novamente.

Privilégios insuficientes para atualizar Este erro normalmente ocorre quando a conta do usuário usada para iniciar a atualização não possui privilégios de acesso à fonte de atualização. Recomendamos certificar-se de que a conta de usuário possui os privilégios necessários. Este erro também pode ser gerado quando há uma tentativa de copiar arquivos de atualização para uma pasta que não pode ser criada.
Erro interno Erro lógico interno na atualização de uma tarefa. Certifique-se de que a configuração das atualizações esteja configurada corretamente e tente novamente.
Erro na verificação de atualizações Este erro é gerado se os arquivos baixados da fonte de atualização não passarem por uma verificação interna. Tente fazer a atualização mais tarde.
ERROS QUE OCORREM QUANDO SE TRABALHA COM ARQUIVOS E PASTAS Esse tipo de erro ocorre quando a conta de usuário usada para executar atualizações possui direitos restritos ou não possui direito para acessar a fonte de atualização ou a pasta onde as atualizações se encontram. Recomendações gerais: Se erros desta natureza ocorrerem, recomendamos verificar se a conta do usuário possui direitos de acesso suficientes para esses arquivos e pastas.
Não é possível criar a pasta Este erro é gerado se uma pasta não puder ser criada durante o procedimento de atualização.
Privilégios insuficientes para executar a operação do arquivo Este erro ocorre se a conta usada para executar a atualização não possui privilégios suficientes para executar operações com os arquivos.
Arquivo ou pasta não encontrados Este erro ocorre se um arquivo ou uma pasta necessária nas atualizações estiver faltando. Recomendamos verificar se o arquivo ou pasta especificada existe e está disponível.
Erro de operação de arquivo Este erro é um erro lógico interno do módulo de atualização durante a execução de operações com arquivos.
ERROS DE REDE Erros neste grupo ocorrem quando existem problemas de conexão ou quando a conexão de rede não está configurada corretamente. Recomendações gerais: Se ocorrerem erros neste grupo, recomendamos certificar-se de que seu computador esteja conectado à Internet, que as configurações da conexão estejam corretamente configuradas, e que a fonte de atualização esteja disponível. Tente então fazer a atualização novamente. Se o problema persistir, contate o Suporte Técnico.
Erro de rede Um erro foi gerado durante a recuperação de arquivos de atualização. Se você encontrar este erro, verifique a conexão de rede do seu computador.
Conexão interrompida Este erro ocorre quando a conexão com a fonte de atualização é encerrada pelo servidor de atualizações por qualquer motivo.

Tempo limite da operação de rede

Tempo limite da conexão da fonte de atualização. Ao ajustar as configurações da atualização do programa, você pode ter que definir um valor baixo de tempo limite para a conexão com a fonte de atualização. Se o seu computador não puder se conectar ao servidor ou à pasta de atualização durante esse tempo, o programa irá retornar este erro. Neste caso, recomendamos que você verifique se as configurações para o Atualizador estão corretas e se a fonte de atualização está disponível.

Erro de autorização no servidor FTP

Este erro ocorre se as configurações de autorização para o servidor FTP usadas como a fonte de atualização forem inseridas incorretamente. Certifique-se de que as configurações atuais do servidor FTP permitam a essa conta de usuário baixar arquivos.

Erro de autorização no servidor proxy

Este erro é gerado se as configurações para a atualização por meio de um servidor proxy indicam incorretamente o nome e senha, ou se a conta de usuário com a qual as atualizações são executadas não possui privilégios de acesso para a fonte de atualização. Edite as configurações de autorização e tente fazer a atualização novamente.

Erro ao verificar o nome DNS

Este erro é gerado se nenhuma fonte de atualização for detectada. É possível que o endereço da fonte de atualização esteja indicado incorretamente, as configurações da rede estejam incorretas, ou o servidor DNS esteja indisponível. Recomendamos que você verifique suas configurações de atualização e disponibilidade das fontes de atualização, e então tente novamente.

A conexão para a fonte de atualização não pôde ser estabelecida

Este erro ocorre se não houver conexão com a fonte de atualização. Certifique-se de que as configurações da fonte das atualizações estejam configuradas corretamente e tente novamente.

A conexão com o servidor proxy não pôde ser estabelecida

Este erro é gerado se as configurações das conexões do servidor proxy estiverem indicadas incorretamente. Para solucionar o problema, recomendamos que você se certifique de que as configurações estejam corretas, que o servidor proxy esteja disponível e que a Internet esteja disponível, e então tente atualizar novamente.

Erro ao verificar o nome DNS do servidor proxy

Este erro é gerado se o servidor proxy não for detectado. Recomendamos certificar-se que as configurações do servidor proxy estejam corretas e que o servidor DNS esteja disponível.

ERROS RELACIONADOS A BANCOS DE DADOS CORROMPIDOS

Esses erros estão conectados a arquivos corrompidos na fonte de atualização.

Recomendações gerais:

Se você estiver fazendo a atualização a partir dos servidores web do Kaspersky Lab, tente fazer a atualização novamente. Se o problema persistir, contate o Suporte Técnico.

Se você estiver atualizando de uma fonte diferente, tal como uma pasta local, nós recomendamos a atualização a partir dos servidores do Kaspersky Lab na Internet. Se o erro ocorrer novamente, contate o Suporte Técnico do Kaspersky Lab.

Arquivo não encontrado na fonte de atualização

Todos os arquivos baixados e instalados no seu computador durante o processo de atualização são listados em um arquivo especial incluído na atualização. Este erro ocorre se existirem quaisquer arquivos na lista de atualização que não se encontrem na fonte de atualização.

Erro na verificação da assinatura

Este erro pode ser retornado pelo aplicativo se a assinatura digital eletrônica do pacote de atualização sendo baixado estiver corrompida ou se não corresponder à assinatura do Kaspersky Lab.

Arquivo de índice corrompido ou faltando

Esse erro é gerado se o arquivo de índice no formato .xml usado para a atualização estiver faltando na fonte de atualização ou estiver corrompido.

ERROS RELACIONADOS À ATUALIZAÇÃO USANDO KASPERSKY ADMINISTRATION KIT ADMINISTRATION SERVER Estes erros são gerados em associação com problemas na atualização do aplicativo através do Kaspersky Administration Kit Administration Server. Recomendações gerais: Primeiro, certifique-se de que o Kaspersky Administration Kit e seus componentes (Administration Server e Network Agent) estejam instalados e operantes. Tente fazer a atualização novamente. Se isso falhar, reinicie o Network Agent e Administration Server e tente a atualização novamente. Se isso não resolver o problema, contate o Suporte Técnico.
Erro ao conectar ao Servidor Administrativo Esse erro é gerado se uma conexão ao Kaspersky Administration Kit Administration Server não puder ser feita. Recomendamos certificar-se de que o NAgent esteja instalado e operante.
Erro de registro no NAgent Se esse erro ocorrer, siga as recomendações gerais para resolver este tipo de erro. Se o erro ocorrer novamente, envie o arquivo de relatório detalhado para a atualização ou Agente de Rede naquele computador ou ao Serviço de Suporte Técnico usando o formulário online. Descreva a situação com detalhes.
A conexão não pode ser estabelecida. O Servidor Administrativo está ocupado e não pode processar o pedido Neste caso, a atualização deve ser tentada posteriormente.
Uma conexão com o Servidor Administrativo / Servidor Administrativo Principal / NAgent, não pôde ser estabelecida, erro físico / erro desconhecido Se você encontrar tais erros, recomendamos que tente fazer a atualização posteriormente. Se o problema persistir, contate o Suporte Técnico.
Erro ao recuperar arquivo do Servidor Administrativo, argumento de transporte inválido Se o erro persistir, contate o Suporte Técnico.
Erro ao recuperar arquivo do Servidor Administrativo Se você encontrar tais erros, recomendamos que tente fazer a atualização posteriormente. Se o problema persistir, contate o Suporte Técnico.
VÁRIOS CÓDIGOS Este grupo inclui erros que não podem ser incluídos em nenhum dos grupos listados acima.
Arquivos para operação de retomada não encontrados Este erro é gerado se outra tentativa de reversão foi feita após completar a retomada das atualizações, mas nenhuma atualização foi feita entre elas. O procedimento de retomada não pode ser repetido até que uma atualização realizada com sucesso, que restaure um conjunto de arquivos de backup tenha sido feita.

CONFIGURAÇÃO DAS CONFIGURAÇÕES DO APLICATIVO

A janela das configurações do aplicativo é usada para acesso rápido às configurações principais do Kaspersky Anti-Virus 6.0.
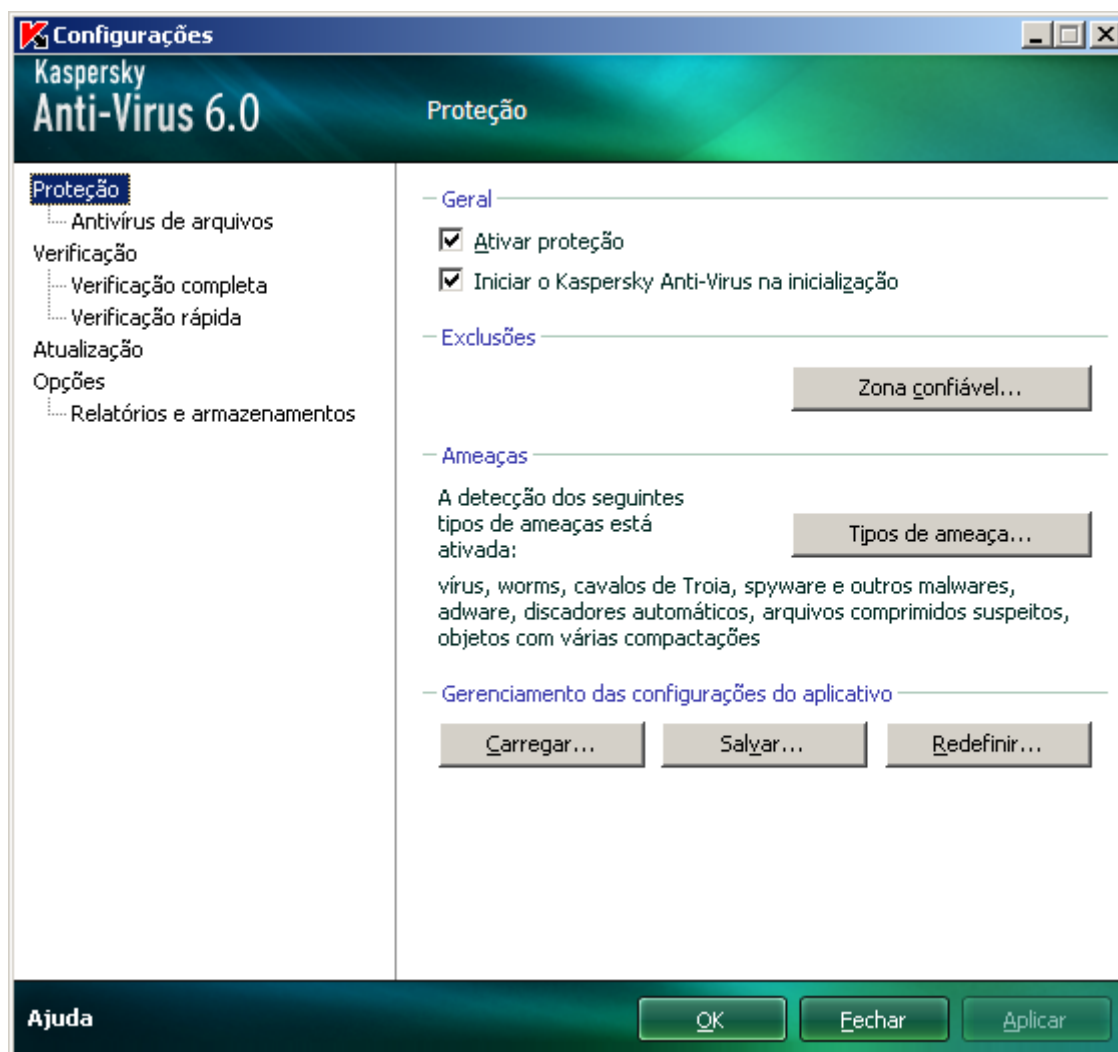
Figura 9. Janela de configuração do aplicativo

A janela consiste de duas partes:

- a parte esquerda da janela dá acesso aos componentes do Antivírus de arquivos, às tarefas de verificação de vírus, às tarefas de atualização etc.;
- a parte direita da janela contém uma lista de configurações do componente, tarefa etc. selecionada na parte esquerda da janela.

Você pode abrir essa janela:

- da janela principal do aplicativo. Para tanto, clique no botão **Configurações** na parte superior da janela principal.

- do menu de contexto. Para fazê-lo, selecione o item **Configurações** no menu de contexto do aplicativo.
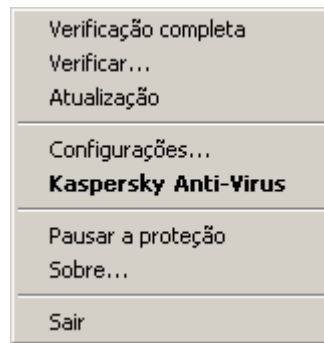
Figura 10. Menu de contexto

NESTA SEÇÃO

PROTEÇÃO

Na janela **Proteção**, você pode usar as seguintes funções adicionais do Kaspersky Anti-Virus:

- Ativando / desativando a proteção do aplicativo (veja página 71).
- Iniciando o aplicativo na inicialização do sistema operacional (veja página 72).
- Selecionando as categorias de ameaças detectáveis (veja página 72).
- Criando uma zona de confiança (veja página 73):
  - criando uma regra de exclusão (veja página 73);
  - criando uma lista de aplicativos de confiança (veja página 75);
  - exportando / importando componentes da zona de confiança (veja página 76).
- Exportando / importando configurações do aplicativo (veja página 77).
- Restaurando as configurações-padrão do aplicativo (veja página 77).

ATIVANDO / DESATIVANDO A PROTEÇÃO DO COMPUTADOR

Por padrão, o Kaspersky Anti-Virus é iniciado quando o sistema operacional é carregado, e protege o seu computador até que este seja desligado. O Antivírus de arquivos está em execução.

Você pode desativar toda a proteção oferecida pelo Antivírus de arquivos.

A Kaspersky Lab recomenda enfaticamente que você **não desative a proteção**, pois isso poderia levar a uma infecção do computador e à perda de dados.

Como resultado da desativação da proteção, o Antivírus de arquivos será interrompido. A desativação dos componentes de proteção não afeta a execução das tarefas de verificação de vírus e atualizações do Kaspersky Anti-Virus.

Para desativar a proteção completamente:

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Desmarque a caixa ☑ **Habilitar proteção**.

INICIANDO O APLICATIVO NA INICIALIZAÇÃO DO SISTEMA OPERACIONAL

Se você tiver que fechar o Kaspersky Anti-Virus completamente por qualquer razão, selecione o item **Sair** no menu de contexto do aplicativo. Então, o aplicativo será descartado da RAM. Isso significa que o computador estará operando desprotegido.

Você pode ativar a proteção do computador iniciando o aplicativo a partir do menu **Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0**.

Também é possível reiniciar a proteção automaticamente depois de reiniciar o sistema operacional.

Para ativar o modo de iniciação do aplicativo na inicialização do sistema operacional, faça o seguinte:

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Marque a caixa ☑ **Executar o Kaspersky Anti-Virus ao iniciar**.

SELECIONANDO AS CATEGORIAS DE AMEAÇAS DETECTÁVEIS

O Kaspersky Anti-Virus o protege contra vários tipos de programas maliciosos. Independentemente das configurações selecionadas, o aplicativo sempre irá verificar e desinfetar vírus e cavalos de Troia. Esses programas podem causar danos significativos ao computador. Para ter mais segurança no seu computador, você pode aumentar a lista de ameaças a serem detectadas, ativando o controle de vários programas possivelmente perigosos.

Para selecionar as categorias de ameaças detectáveis:

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Ameaças**, clique o botão **Tipos de ameaças**.
4. Na janela **Tipos de ameaças** que irá se abrir, marque as ☑ caixas para as categorias de ameaças contra as quais você quer proteger seu computador.

CRIANDO UMA ZONA DE CONFIANÇA

A zona de confiança é uma lista de objetos criada pelo usuário, que o Kaspersky Anti-Virus não monitora. Em outras palavras, é um conjunto de exclusões a partir do escopo de proteção do aplicativo.

O usuário cria uma zona de confiança baseada nas características dos objetos que ele ou ela trabalha e nos aplicativos instalados no computador do usuário. Você pode precisar criar tal lista de exclusão se, por exemplo, o Kaspersky Anti-Virus bloquear acesso a um objeto ou aplicativo que você tem certeza que é absolutamente seguro.

Você pode excluir da verificação arquivos de certos formatos, usar uma máscara de arquivo, ou excluir certa área (por exemplo, uma pasta ou aplicativo), processos de programas, ou objetos de acordo com a classificação da Enciclopédia de vírus (status dados a objetos pelo Kaspersky Anti-Virus durante uma verificação).

Um objeto de exclusão é excluído do verificação quando o disco ou a pasta onde ele está localizado é verificado. Entretanto, se você selecionar especificamente aquele objeto, a regra de exclusão não será aplicada a ele.

Para criar uma lista de exclusões da verificação, faça o seguinte:

1. Abra o janela das configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Exclusões**, clique no botão **Zona confiável**.
4. Na janela que irá se abrir, configure as regras de exclusão para objetos (veja página 73), e crie uma lista de aplicativos confiáveis (veja página 75).

CONSULTE TAMBÉM:

CRIANDO UMA REGRA DE EXCLUSÃO

As regras de exclusão são conjuntos de condições que o Kaspersky Anti-Virus usa para verificar se ele pode pular ao verificação de um objeto.

Você pode excluir da verificação arquivos de certos formatos, usar uma máscara de arquivo, ou excluir certa área (por exemplo, uma pasta ou aplicativo), processos de programas, ou objetos de acordo com a classificação da Enciclopédia de vírus.

Tipo de ameaça é o status que o Kaspersky Anti-Virus atribui a um objeto durante sua verificação. Este status é dado baseado na classificação de malware e riskware achados na Enciclopédia de vírus do Kaspersky Lab.

Software potencialmente perigosos não possuem funções maliciosas, mas podem ser usados como um componente auxiliar para um código pernicioso, uma vez que eles contêm buracos e erros. Esta categoria inclui, por exemplo, aplicativos administrativos remotos, clientes IRC, servidores FTP, utilitários de múltiplas finalidades, keyloggers (registradores de teclado), macros de senhas, discadores automáticos etc. Tal software é classificado como não vírus, mas pode ser dividido em vários tipos, ex. Adware, Joke, Riskware, etc. (para mais informações sobre softwares potencialmente perigosos detectados pelo Kaspersky Anti-Virus, consulte a Enciclopédia de vírus no endereço www.viruslist.com (http://www.viruslist.com/en/viruses/encyclopedia)). Depois da verificação, esses programas podem

ser bloqueados. Uma vez que muitos deles são grandemente explorados por usuários, eles podem ser excluídos da verificação. Para tanto, você deve adicionar o nome da ameaça ou a máscara do nome da ameaça (de acordo com a classificação da Enciclopédia de vírus) para a zona de confiança.

Por exemplo, talvez você use com frequência o programa Administração remota. Este é um sistema de acesso remoto que permite que você opere suas fontes de um computador remoto. O Kaspersky Anti-Virus vê este tipo de atividade de aplicativos como potencialmente perigosa e pode bloqueá-la. Para evitar o bloqueio do aplicativo, você deve criar uma regra de exclusão que especificaria o Remote Admin como o veredicto.

Quando uma exclusão for adicionada, produz uma regra que também pode ser usada pelo Antivírus de arquivos e na execução detarefas de verificação de vírus.

➡ *Para criar uma regra de exclusão:*

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Exclusões**, clique no botão **Zona confiável**.
4. Na janela que irá se abrir, na aba **Regras de exclusão**, clique no botão **Adicionar**.
5. Na janela de **Máscara de exclusão** que se abre, na seção **Propriedades**, selecione um tipo de exclusão. Então, na seção **Descrição da regra**, dê valores aos tipos de exclusão selecionados e selecione quais componentes do Kaspersky Anti-Virus devem ser cobertos pela regra.

➡ *Para criar uma regra de exclusão da janela de relatório, faça o seguinte:*

1. Selecione o objeto do relatório para adicionar às exclusões.
2. Selecione o item **Adicionar à zona confiável** do menu de contexto para este objeto.
3. Na janela **Máscara de exclusão** que será aberta, verifique que esteja satisfeito com as configurações das regras de exclusão. Os campos Nome do objeto e tipo de ameaça relevante são preenchidos automaticamente, baseados em dados do relatório. Para criar uma regra, clique no botão **OK**.

MÁSCARAS DE EXCLUSÃO DE ARQUIVOS PERMITIDOS

Vamos examinar mais detalhadamente alguns exemplos de máscaras permitidas que você pode usar ao criar a lista de arquivos a serem excluídos da verificação:

1. Máscaras sem caminhos de arquivos:
   - ***.exe** – todos os arquivos com a extensão *.exe*;
   - ***.ex?** – todos os arquivos com a extensão *ex?* onde *?* pode representar qualquer caractere único;
   - **teste** – todos os arquivos com o nome *teste*.
2. Máscaras com caminhos de arquivos absolutos:
   - **C:\dir*.***, **C:\dir*** ou **C:\dir** – todos os arquivos da pasta *C:\dir*;
   - **C:\dir*.exe** – todos os arquivos com a extensão .exe na pasta *C:\dir*;
   - **C:\dir*.ex?** – todos os arquivos com a extensão *ex?* na pasta *C:\dir*, onde *?* pode representar qualquer caractere;
   - **C:\dir\teste** – somente o arquivo *C:\dir\teste*.

   Se não desejar que o aplicativo verifique os arquivos em todas as subpastas armazenadas na pasta especificada, marque a caixa ☑ **Incluir subpastas** ao criar a máscara.

3. Máscaras de caminhos de arquivos:

   - **dir*.***, **dir*** ou **dir** – todos os arquivos em todas as pastas *dir*\;
   - **dir\teste** – todos os arquivos *teste* nas pastas *dir*\;
   - **dir*.exe** – todos os arquivos com a extensão *.exe* em todas as pastas *dir*\;
   - **dir*.ex?** – todos os arquivos com a extensão *ex?* em todas as pastas *dir*\, onde *?* pode representar qualquer caractere.

     Se não desejar que o aplicativo verifique os arquivos em todas as subpastas armazenadas na pasta especificada, marque a caixa ☑ **Incluir subpastas** ao criar a máscara.

As máscaras de exclusão *.* e * poderão ser usadas somente se você especificar o tipo de classificação da ameaça de acordo com a Enciclopédia de vírus. Nesse caso, a ameaça especificada não será detectada em nenhum objeto. Ao usar essas máscaras sem especificar o tipo de classificação, o monitoramento é desativado. Além disso, ao configurar uma exclusão, não é recomendável selecionar um caminho relacionado a um disco de rede criado com base em uma pasta do sistema de arquivos usando o comando subst ou a um disco que espelha uma pasta de rede. Recursos diferentes podem receber o mesmo nome de disco para usuários diferentes, o que levaria, inevitavelmente, a um acionamento incorreto das regras de exclusão.

CONSULTE TAMBÉM:

Máscaras de exclusões permitidas de acordo com a Enciclopédia de vírus 75

MÁSCARAS DE EXCLUSÕES PERMITIDAS DE ACORDO COM A ENCICLOPÉDIA DE VÍRUS

Ao adicionar máscaras para excluir determinadas ameaças de acordo com sua classificação na Enciclopédia de vírus, você pode especificar:

- o nome complete da ameaça, conforme dado na Enciclopédia de vírus em www.viruslist.com p. ex., **um não-vírus:RiskWare.RemoteAdmin.RA.311** ou **Flooder.Win32.Fuxx**;
- o nome da ameaça por máscara, por exemplo:
  - **not-a-virus*** – exclui da verificação programas legais mas possivelmente perigosos, além de programas de piadas;
  - ***Riskware.*** – exclui da verificação os riskware;
  - ***RemoteAdmin.*** – exclui da verificação todos os programas de administração remota.

CONSULTE TAMBÉM:

Máscaras de exclusão de arquivos permitidos 74

CRIANDO UMA LISTA DE APLICATIVOS CONFIÁVEIS

Você pode criar uma lista de aplicativos confiáveis. A atividade de tais programas, incluindo atividade suspeita, atividade de arquivo, atividade de rede e tentativas de acesso ao registro do sistema não serão monitoradas.

Por exemplo, você pode achar que os objetos usados pelo **Bloco de notas** da Microsoft Windows são seguros e não precisam ser verificados. Em outras palavras, você confia nesse aplicativo. Para excluir os objetos usados por este processo do verificação, adicione o aplicativo **Bloco de notas** à lista de aplicativos confiáveis. Ao mesmo tempo, o arquivo executável e o processo do aplicativo confiável serão verificados quanto à presença de vírus, como anteriormente. Para excluir totalmente um aplicativo da verificação, você deve usar regras de exclusão.

Além disso, algumas ações classificadas como perigosas podem ser executadas normalmente por vários aplicativos. Por exemplo, aplicativos que alternam automaticamente o layout do teclado, como o Punto Switcher, normalmente interceptam o texto inserido no teclado. Para considerar as especificidades desses aplicativos e desativar o monitoramento de suas atividades, é recomendável adicioná-los à lista de aplicativos confiáveis.

Ao utilizar a exclusão de aplicativos confiáveis, você também pode resolver conflitos de compatibilidade potenciais entre o Kaspersky Anti-Virus e outros aplicativos (por exemplo, tráfego de rede de outro computador que já foi verificado pelo antivírus) e pode aumentar a produtividade do computador, o que é especialmente importante ao usar aplicativos de servidor.

Por padrão, o Kaspersky Anti-Virus verifica objetos sendo abertos, executados ou salvos por qualquer processo de programa, e monitora a atividade de todos os aplicativos e o tráfego de rede que eles criam.

➡ *Para adicionar um aplicativo à lista confiável:*

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Exclusões**, clique no botão **Zona confiável**.
4. Na janela que irá se abrir, na aba **Aplicativos confiáveis**, clique no botão **Adicionar**.
5. Na janela **Aplicativo confiável** que irá se abrir, selecione o programa clicando no botão **Procurar**. Um menu de contexto irá se abrir; clicando no item **Procurar**, você pode ir para a janela de seleção do arquivo padrão e selecionar o caminho para o arquivo executável, ou clicando o item **Aplicativos**, você pode alternar para a lista de aplicativos sendo executados no momento, e selecionar um deles ou mais, se necessário. Especifique as configurações necessárias para o aplicativo selecionado.

EXPORTANDO / IMPORTANDO COMPONENTES DA ZONA DE CONFIANÇA

Usando exportar e importar, é possível transferir a lista criada de regras de exclusão e aplicativos confiáveis para outros computadores.

➡ *Para copiar as regras de exclusão, faça o seguinte:*

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Exclusões**, clique no botão **Zona confiável**.
4. Na janela que se abre, na aba **Regras de exclusão**, use os botões **Exportar** e **Importar** para executar as ações requeridas para copiar as regras.

➡ *Para copiar a lista de aplicativos confiáveis, faça o seguinte:*

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Exclusões**, clique no botão **Zona confiável**.
4. Na janela que se abre, na aba **Aplicativos confiáveis**, use os botões **Exportar** e **Importar** para executar as ações requeridas para copiar a lista.

EXPORTANDO / IMPORTANDO AS CONFIGURAÇÕES DO KASPERSKY ANTI-VIRUS

O Kaspersky Anti-Virus fornece a opção de importar e exportar suas configurações.

Esta função é útil quando, por exemplo, o aplicativo é instalado no seu computador doméstico e no seu escritório. Você pode configurar o aplicativo da forma que quiser em casa, exportar essas configurações como um arquivo em um disco e carregá-las no seu computador do trabalho usando a função Importar. As configurações são armazenadas em um arquivo de configuração especial.

Para exportar as configurações atuais do aplicativo, faça o seguinte:

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Gerenciamento das configurações do aplicativo**, clique no botão **Salvar**.
4. Na janela que será aberta, insira o nome do arquivo de configuração e o caminho no qual ele deve ser salvo.

Para importar as configurações do aplicativo a partir de um arquivo de configuração armazenado, faça o seguinte:

1. Abra a janela de configuraçãodo aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Gerenciamento das configurações do aplicativo**, clique no botão **Carregar**.
4. Na janela que se abre, selecione um arquivo do qual você deseja importar as configurações do Kaspersky Anti-Virus.

RESTAURANDO AS CONFIGURAÇÕES PADRÃO

Você sempre pode retornar às configurações de fábrica ou as configurações recomendadas do Kaspersky Anti-Virus. Elas são consideradas ideais e são recomendadas pela Kaspersky Lab. O Assistente de configuração do aplicativo restaura as configurações de fábrica.

Na janela que será aberta, você terá a opção de especificar que configurações devem ou não ser salvas junto com a restauração do nível de segurança exigido.

Depois de concluir o Assistente, o nível de segurança **Recomendado** será configurado para o Antivírus de arquivos, levando em conta as configurações que você decidiu manter intatas na restauração. Além disso, as configurações especificadas ao trabalhar com o assistente também serão aplicadas.

Para restaurar as configurações de proteção:

1. Abra a janelade configurações do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Proteção**.
3. Na seção **Gerenciamento de configurações do aplicativo**, clique no botão **Reset**.
4. Na janela que será aberta, marque as caixas das configurações que devem ser salvas. Clique no botão **Avançar**. O Assistente de configuração inicial será inicializado; siga suas instruções.

ANTIVÍRUS DE ARQUIVOS

As configurações do componente do **Antivírus de arquivo** são agrupadas na janela (ver seção "Proteção do antivírus do sistema de arquivos do computador" na página 37). Ao editar as configurações do aplicativo, você pode:

- alterar o nível de segurança (veja página 39);
- alterar a ação tomada ou objetos detectados (veja página 39);
- criar um escopo de proteção (veja página 40);
- otimizar o verificação (veja página 42);
- configurar o verificação de arquivos compostos (veja página 42);
- mudar o modo de verificação (veja página 43);
- usar a análise heurística (veja página 41);
- pausar o componente (veja página 44);
- selecionar uma tecnologia de verificação (veja página 43);
- restaurar as configurações de proteção de fábrica (veja página 45) se elas tiverem sido modificadas.

➡ *Para continuar configurando o Antivírus de arquivos:*

1. Abra a janela de configuração do aplicativo.
2. Na parte esquerda da janela, selecione a seção **Antivírus de arquivo**.
3. À direita da janela, selecione as configurações do componente referentes ao nível de segurança e à reação à ameaça. Clique no botão **Personalizar** para alternar para outras configurações do Antivírus de arquivo.

VERIFICAÇÃO

A seleção do método a ser usado para verificar objetos no seu computador é determinada por um conjunto de propriedades designadas para cada tarefa.

Os especialistas do Kaspersky Lab distinguem várias tarefas de verificação de vírus. Elas são as seguintes:

Verificação

Verificação de objetos selecionados pelo usuário. Você pode verificar qualquer objeto do sistema de arquivos do computador.

Verificação completa

Uma verificação completa de todo o sistema. Os seguintes objetos são verificados por padrão: memória do sistema, programas carregados na inicialização, backup do sistema, bancos de dados de email, discos rígidos, mídias de armazenamento removíveis e unidades de rede.

Verificação rápida

Verificação de vírus nos objetos de inicialização do sistema operacional.

A janela de configurações de cada tarefa permite que você faça o seguinte:

- selecionar o nível de segurança (veja página 50) com as configurações que a tarefa irá usar;

- selecionar uma ação (veja página 50) que o aplicativo irá tomar quando ele detectar um objeto infectado / potencialmente infectado;
- criar uma agenda (veja página 56) para executar tarefas automaticamente;
- especificar os tipos de arquivo (veja página 51) para serem verificados para vírus;
- configurar as configurações de scan para arquivos compostos (veja página 53);
- selecionar os métodos de verificação e as tecnologias de verificação (veja página 54);
- definir as configurações comuns de verificação para todas as tarefas (veja página 58).

Para editar as configurações de tarefas:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Verificação** (**Verificação completa**, **Verificação rápida**).
3. No lado direito da janela, selecione o nível de segurança requerido, a reação à ameaça e configure o modo de execução. Clique no botão **Personalizar** para alterar as configurações das configurações de outras tarefas. Para restaurar as configurações padrão, clique no botão do **nível Padrão**.

ATUALIZAÇÃO

A atualização do Kaspersky Anti-Virus é executada usando as configurações para determinar o seguinte:

- a fonte (veja página 61) da qual as atualizações serão baixadas e instaladas;
- (veja página 64) e os componentes específicos a serem atualizados (veja página);
- com que regularidade a atualização será executada se a execução programada for configurada (veja página 63);
- em que conta (veja página 63) a atualização será executada;
- se as atualizações forem copiadas para uma fonte local (veja página 65);
- uso de um servidor proxy (veja página 62).

Para realizar a atualização da configuração:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Atualização**.
3. Selecione o modo de execução requerido à direita da janela. Clique no botão **Configurar** para poder configurar outras tarefas.

OPÇÕES

Na janela **Opções**, você pode usar as seguintes funções adicionais do Kaspersky Anti-Virus:

- Autodefesa do aplicativo (veja página 80).
- Restringindo o acesso ao aplicativo (veja página 80).
- Limitando o tamanho dos arquivos de iSwift files (veja página 81).

- Desempenho do servidor ao usar a configuração de vários processadores.(veja página 81).
- Notificações sobre eventos do Kaspersky Anti-Virus (veja página 82):
  - selecionando o tipo de evento e a forma de enviar notificações (veja página 82);
  - configurando notificação de email (veja página 83);
  - configurando o registro de eventos (veja página 83).
- elementos ativos de interface (veja página 84).

AUTODEFESA DE APLICATIVOS

O Kaspersky Anti-Virus garante a segurança do computador contra malware e, por isso, ele próprio pode ser alvo de programas maliciosos que tentam bloqueá-lo ou excluí-lo.

Para verificar a estabilidade do sistema de segurança do computador, o aplicativo tem seus próprios mecanismos de autodefesa e proteção contra acesso remoto.

➡ *Para permitir os mecanismos de autodefesa do Kaspersky Anti-Virus:*

1. Abra a janela de configuração dodo aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Na seção **Autodefesa**, marque a caixa ☑ **Ativar Autodefesa** para instalar os mecanismos de proteção do Kaspersky Anti-Virus contra alteração ou exclusão de seus próprios arquivos do disco rígido, de processos da RAM e dos registros do sistema.

   Na seção **Autodefesa**, marque a caixa ☑ **Desativar controle de serviços externos** para bloquear quaisquer tentativas de gerenciar os serviços do aplicativo remotamente.

   Se houver alguma tentativa de executar as ações listadas, aparecerá uma mensagem sobre o ícone do aplicativo na área de notificação da barra de tarefas (a menos que o serviço de notificação tenha sido desativado pelo usuário).

RESTRIÇÃO DE ACESSO AO APLICATIVO

Seu computador pessoal pode ser usado por várias pessoas com níveis diferentes de experiência em informática. Permitir o acesso ao Kaspersky Anti-Virus e a suas configurações pode diminuir bastante a segurança do computador como um todo.

Para aumentar o nível de segurança do computador, use uma senha de acesso ao Kaspersky Anti-Virus. Isso pode bloquear todas as operações, exceto as notificações de detecção de objetos perigosos, e evitar que as seguintes ações sejam executadas:

- alteração das configurações do aplicativo;
- encerramento do aplicativo;
- desativar o Antivírus de arquivos e as tarefas de verificação;
- política de desativação (quando os aplicativos estão funcionando via o Kit de Administração do Kaspersky);
- remoção do aplicativo.

Cada uma dessas ações listadas acima reduz o nível de proteção do computador; assim, tente estabelecer quais usuários são confiáveis para executá-las.

Para proteger o acesso ao aplicativo com uma senha:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Na seção **Proteção por senha**, marque a caixa ☑ **Ativar proteção por senha** e clique no botão **Configurações**.
4. Na janela **Proteção por senha** que será aberta, digite a senha e especifique a área a ser coberta por restrição de acesso. Agora, sempre que um usuário do computador tentar executar as ações selecionadas, o aplicativo sempre solicitará a senha.

RESTRINGINDO O TAMANHO DE ARQUIVOS ISWIFT

Os *arquivos iSwift* são aqueles que contêm informações sobre objetos NTFS já verificados quanto a vírus (tecnologia iSwift). O uso desses arquivos permite aumentar a velocidade da verificação enquanto o Kaspersky Anti-Virus verifica apenas os objetos modificados desde a última verificação. Com o tempo, o tamanho dos arquivos iSwift aumenta. Recomendamos que você restrinja o tamanho desses arquivos. Quando o seu valor for atingido, o iSwift-file será limpo.

Para limitar o tamanho dos arquivos iSwift:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Na seção **Recursos**, marque a caixa ☑ **Reinicializar banco de dados iSwift ao chegar** e especifique o tamanho do banco de dados em MB próximo a ele.

CONFIGURAÇÃO DO SERVIDOR DE VÁRIOS PROCESSADORES

Quando usar a configuração de vários processadores, você pode gerenciar o desempenho do servidor nas seguintes formas:

- Definir o número de cópias do kernel antivírus a ser carregado quando o Kaspersky Anti-Virus estiver sendo executado no servidor (ou seja, o número de processos antivírus em execução no servidor em paralelo).

  Quanto mais cópias do kernel antivírus estiverem em execução, maior será a velocidade em que os objetos serão processados pelo antivírus. Porém, isso afeta o desempenho geral do servidor. Podem ocorrer falhas na operação do Antivírus de arquivos se o volume RAM for insuficiente ou se uma grande quantidade de cópias do kernel antivírus estiver em execução.

  Além disso, vários processos antivírus em execução no servidor simultaneamente garantem a proteção contínua do servidor em caso de falha do kernel.

- Controlar a carga do servidor: por exemplo, reservar uma seção do processador para o processamento antivírus dos objetos e outra seção para as tarefas principais do servidor.

  A Kaspersky Lab recomenda reservar pelo menos um processador para as tarefas do servidor quando estiver operando um servidor de vários processadores.

Para definir o número de cópias do kernel antivírus:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Na seção **Configuração de várias CPUs**, pressione o botão **Detalhes**.

4. Na janela **Configuração de várias CPUs** que será aberta, na seção **Parâmetros**, especifique o número de cópias do kernel antivírus.

Para equilibrar a carga do servidor:

1. Abra a janela de configuraçãodo aplicativo.
2. À esquerda da janela, selecione a seção Opções.
3. Na seção Configuração de várias CPUs, pressione o botão Detalhes.
4. Na janela **Configuração de várias CPUs** que será aberta, na seção **Processadores utilizados**, desmarque as caixas ☑ para processadores que devem ser reservados estritamente para a operação do servidor.

NOTIFICAÇÕES SOBRE EVENTOS DO KASPERSKY ANTI-VIRUS

Diferentes tipos de eventos ocorrem durante a operação do Kaspersky Anti-Virus. Eles podem ser de natureza de referência ou conter informações importantes. Por exemplo, um evento pode informá-lo sobre a conclusão bem-sucedida de uma atualização do aplicativo ou pode registrar um erro na operação de um determinado componente que deve ser corrigido imediatamente.

Para ficar atualizado com os eventos mais recentes na operação do Kaspersky Anti-Virus, use o recurso notificação.

As notificações podem ser entregues das seguintes formas:

- mensagens pop-up que aparecem acima do ícone do aplicativo na bandeja do sistema;
- notificação sonora;
- mensagens de email;
- gravando informações no registro de eventos.

Para usar o serviço de notificação, faça o seguinte:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Na seção **Aparência**, marque a caixa ☑ **Ativar notificações** e clique no botão **Configurações**.
4. Na janela de **Configurações de notificação** que será aberta, especifique os tipos de eventos do Kaspersky Anti-Virus sobre os quais você quer receber notificação, bem como os tipos de notificação.

CONSULTE TAMBÉM:

SELECIONANDO O TIPO DE EVENTO E A FORMA DE ENVIAR NOTIFICAÇÕES

Durante a execução do Kaspersky Anti-Virus, surgem os seguintes tipos de eventos:

- **Notificações críticas** são eventos de importância crítica. É altamente recomendado que elas sejam relatadas com as notificações já que apontam para problemas na operação do aplicativo ou lacunas de proteção do computador. Por exemplo, *os bancos de dados estão obsoletos* ou *o prazo de validade da licença expirou*.

- **Notificações de erro** são eventos que levam à não-funcionalidade do aplicativo. Por exemplo, *bancos de dados estão faltando ou estão corrompidos*.

- **Notificações importantes** são eventos que devem ser observados pois refletem situações importantes na operação do aplicativo. Por exemplo, *os bancos de dados estão obsoletos* ou *a licença expira em breve*.

- **Notificações secundárias** são mensagens de tipo de referência que não contêm informações importantes, como regra. Por exemplos, *objeto posto em quarentena*.

Para especificar quais eventos o aplicativo deve notificar e como, faça o seguinte:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Na seção **Aparência**, marque a caixa ☑ **Ativar notificações** e clique no botão **Configurações**.
4. Na janela **Configurações de Notificação** que abrirá, marque as ☑ caixas para os eventos e as formas de enviar notificações para eles, das quais você deseja receber notificações.

CONFIGURANDO NOTIFICAÇÃO POR EMAIL

Depois de ter selecionado os eventos (consulte a seção "Selecionando tipo de evento e forma de enviar notificações" na página 82) dos quais deseja receber notificação por email, você deve configurar notificações.

Para configurar notificações de email faça o seguinte:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Na seção **Aparência**, marque a caixa ☑ **Ativar notificações** e clique no botão **Configurações**.
4. Na janela **Configurações de Notificação** que abrirá, marque as ☑ caixas para os eventos requeridos no campo **Email** e clique no botão **Configurações de email**.
5. Na janela **Configurações de notificação de email** que se abrirá, especifique os valores requeridos para as configurações. Se você deseja que notificações sobre eventos sejam enviadas em horas programadas, crie uma programação de envio de mensagens informativas clicando no botão **Alterar**. Faça as mudanças necessárias na janela **Programar** que irá se abrir.

CONFIGURANDO O REGISTRO DE EVENTOS

O Kaspersky Anti-Virus fornece a opção de registrar informações sobre eventos que ocorrem enquanto o aplicativo está sendo executado, no registro geral de eventos do Microsoft Windows (**Aplicativo**) ou em um registro de eventos dedicado do Kaspersky Anti-Virus (**Log de eventos Kaspersky**).

Registros podem ser exibidos no **Visualizador de Eventos** do Microsoft Windows que se abrirá usando a opção **Iniciar/Configurações/Painel de Controle/Administração/Exibir Eventos**.

Para configurar o registro de eventos, faça o seguinte:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.

3. Na seção **Aparência**, marque a caixa ☑ **Ativar notificações** e clique no botão **Configurações**.
4. Na janela **Configurações de Notificação** que abrirá, marque as ☑ caixas para os eventos requeridos no campo **Registro** e clique no botão **Configurações de Registro**.
5. Na janela **Configurações do Log de Eventos** que abrirá, selecione o registro em que as informações sobre eventos serão registradas.

ELEMENTOS ATIVOS DA INTERFACE

Elementos ativos da interface incluem as seguintes opções do Kaspersky Anti-Virus:

Ícone animado de área de notificação da barra de tarefas.

Dependendo da operação em execução pelo aplicativo, o ícone do aplicativo na bandeja do sistema mudará. Por exemplo, ao verificar mensagens de email, um pequeno ícone de letra aparecerá na frente do ícone do aplicativo. Por padrão, o ícone do aplicativo está animado. Nesse caso, o ícone exibe apenas o status de proteção do computador: se a proteção estiver ativada, o ícone será colorido; se a proteção estiver pausada ou desativada, o ícone será cinza.

Mostrar Protegido pela Kaspersky Lab na tela de logon do Microsoft Windows.

Por padrão, esse indicador aparece no canto superior direito da tela quando o Kaspersky Anti-Virus é iniciado. Ele informa que o computador está protegido de todos os tipos de ameaça.

➧ *Para configurar os elementos ativos da interface:*

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Opções**.
3. Marque as caixas requeridas na seção **Aparência**.

RELATÓRIOS E ARMAZENAMENTOS

A seção contém as configurações que controlam as operações com arquivos de dados de aplicativos.

Arquivos de dados do aplicativo são objetos que foram colocados na Quarentena pelo Kaspersky Anti-Virus ou movidos para o Backup, além dos arquivos com relatórios sobre a operação de componentes do aplicativo.

Nesta seção, você pode:

- configurar a criação e armazenamento do relatório (veja página 85);
- configure a quarentena e o backup (veja página 88);
- limpe o arquivo do relatório, a Quarentena e o Backup.

➧ *Para limpar áreas de armazenamento:*

1. Abra a janelade configurações do aplicativo.
2. À esquerda da janela, selecione a seção **Relatórios e Armazenamentos**.
3. Na janela que será aberta, clique no botão **Limpar**.
4. Nos janela **Arquivos de dados** que será aberta, especifique as áreas de armazenamento das quais todos os objetos deverão ser removidos.

CONSULTE TAMBÉM:

PRINCÍPIOS DE MANUSEIO DE RELATÓRIOS

A operação do Antivírus de arquivos e a execução de todas as tarefas de verificação e atualização é registrada em um relatório.

➡ *Para exibir os relatórios:*

1. Abra a janela principal do aplicativo.
2. Clique no botão **Relatórios**.

➡ *Para revisar todos os eventos sobre o desempenho de um componente ou de uma tarefa registrada no relatório:*

1. Abra a janela principal do aplicativo e clique no botão botão **Relatórios**.
2. Na janela que será aberta, na aba **Relatórios**, selecione o nome de um componente ou tarefa e clique no link **Detalhes**. Como resultado, uma janela com informação detalhada sobre o Antivírus de arquivos ou a operação da tarefa será aberta. A estatística resultante da execução será exibida à esquerda da janela, e informações detalhadas aparecem nas várias abas da parte central. O conjunto de guias pode variar dependendo de o relatório ter sido selecionado para Antivírus de arquivos ou para uma tarefa.

➡ *Para importar o relatório para um arquivo de texto:*

1. Abra a janela principal de aplicativos e clique no botão **Relatórios**.
2. Na janela que será aberta, na aba **Relatórios**, selecione o nome de um componente ou tarefa e clique no link **Detalhes**.
3. Na janela que será aberta as informações sobre a execução de um componente ou tarefa selecionada serão exibidas. Clique no botão **Salvar como** e especifique onde você deseja salvar o arquivo de relatório.

CONFIGURANDO RELATÓRIOS

Você pode modificar as seguintes definições para criar e salvar os relatórios:

- Permitir ou bloquear o registro de eventos informativos. Como regra, estes eventos não são críticos para a proteção (caixa ☑ **Registrar eventos não críticos**).
- Permitir o registro no relatório apenas dos eventos ocorridos desde a última execução da tarefa. Isso economiza espaço em disco, reduzindo o tamanho do relatório (caixa ☑ **Manter apenas eventos recentes**).

Se a caixa estiver marcada, as informações serão atualizadas sempre que a tarefa for reiniciada. No entanto, apenas as informações não críticas serão substituídas.

- Defina o período de armazenamento dos relatórios (caixa ☑ **Armazenar relatórios por no máximo**). Por padrão, o tempo de armazenamento dos objetos é de 30 dias e, depois disso, eles serão excluídos. Você pode alterar o tempo máximo de armazenamento ou até mesmo cancelar as restrições impostas.
- Especifique o tamanho máximo do relatório (caixa ☑ **Tamanho máximo**). Por padrão, o tamanho máximo é 250 MB. Você pode cancelar as restrições impostas para o tamanho do relatório ou inserir outro valor.

➡ *Para configurar as configurações de armazenamento do relatório, faça o seguinte:*

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Relatórios e Armazenamentos**.
3. Na seção **Relatórios**, marque todas as caixas requeridas, e configure o prazo de armazenamento e o tamanho máximo do relatório, caso necessário.

QUARENTENA DE OBJETOS POSSIVELMENTE INFECTADOS

A **Quarentena** é um repositório especial que armazena os objetos possivelmente infectados por vírus.

Objetos possivelmente infectados são aqueles que se suspeita estarem infectados por vírus ou modificações deles.

Por que *possivelmente infectado*? Nem sempre é possível determinar exatamente se um objeto está infectado. Isto pode acontecer por vários motivos:

- *O código do objeto analisado se parece com uma ameaça conhecida, mas está parcialmente modificado*.

  Os bancos de dados de aplicativos contêm informações sobre as ameaças investigadas até o presente por especialistas do Kaspersky Lab. Se um programa prejudicial foi modificado e essas alterações ainda não foram inseridas no banco de dados, o Kaspersky Anti-Virus classificará o objeto infectado com esse programa prejudicial modificado como possivelmente infectado e indicará com segurança a ameaça com a qual essa infecção se parece.

- *O código do objeto detectado se parece estruturalmente com um programa malicioso; contudo, não há nada semelhante registrado nos bancos de dados do aplicativo*.

  É bastante provável que se trate de um novo tipo de ameaça, então o Kaspersky Anti-Virus classifica esse objeto como possivelmente infectado.

Os arquivos são identificados como possivelmente infectados por um vírus pelo *analisador de código heurístico*. Esse mecanismo é bastante eficiente e raramente produz falsos positivos.

Um objeto possivelmente infectado pode ser detectado e colocado em quarentena na verificação de vírus e pelo Antivírus de arquivos.

Quando um objeto é colocado na Quarentena, ele é movido e não copiado: o objeto é excluído do disco ou do email e salvo na pasta Quarentena. Os arquivos na Quarentena são salvos em um formato especial e não são perigosos.

CONSULTE TAMBÉM:

AÇÕES EM OBJETOS NA QUARENTENA

Você pode executar as seguintes operações com os objetos da Quarentena:

- colocar na Quarentena os arquivos que suspeita estarem infectados;
- verificar e desinfetar todos os objetos possivelmente infectados da Quarentena usando os bancos de dados atuais do aplicativo atual;
- restaurar os arquivos para as pastas das quais foram movidos para a Quarentena ou para as pastas selecionadas pelo usuário;
- excluir qualquer objeto ou um grupo de objetos selecionados da Quarentena.

Para executar ações com os objetos da Quarentena, faça o seguinte:

1. Abra a janela principal do aplicativo e clique no botão **Detectado**.
2. Na janela que será aberta, na aba **Quarentena**, tome as medidas necessárias.

CÓPIAS DE BACKUP DE OBJETOS PERIGOSOS

Às vezes, não é possível manter a integridade dos objetos durante a desinfecção. Se o arquivo desinfetado continha informações importantes e, após a desinfecção, elas ficaram parcial ou totalmente inacessíveis, você poderá tentar restaurar o objeto original a partir de sua cópia de backup.

Uma cópia de backup é uma cópia do objeto perigoso original, criada quando ele é desinfetado ou excluído pela primeira vez e salva no backup.

O backup é um repositório especial que contém cópias de backup de objetos perigosos após o processamento ou a exclusão. A principal função do backup é possibilitar a restauração do objeto original a qualquer momento. Os arquivos do backup são salvos em um formato especial e não são perigosos.

CONSULTE TAMBÉM:

Trabalhando com cópias de backup 87

Configurando a quarentena e o backup 88

TRABALHANDO COM CÓPIAS DE BACKUP

Você pode executar as seguintes operações nos objetos armazenados no backup:

- restaurar cópias selecionadas;
- excluir objetos.

Para executar ações com os objetos do backup, faça o seguinte:

1. Abra a janela principal do aplicativo e clique no botão **Detectado**.
2. Na janela que será aberta, na aba **Backup**, execute as ações necessárias.

CONFIGURANDO A QUARENTENA E O BACKUP

Você pode editar as seguintes configurações da quarentena e do backup:

- Permitir modo de auto verificação para objetos em quarentena após cada atualização da base de dados do aplicativo (a caixa ☑ **Verificar arquivos da Quarentena após a atualização**).

  O Kaspersky Anti-Virus não poderá verificar os objetos da Quarentena imediatamente após a atualização dos bancos de dados do aplicativo se você estiver trabalhando com a Quarentena.

- Determinar o tempo máximo de armazenamento para objetos em quarentena e para cópias de objetos em backup (a caixa ☑ **Armazenar objetos por no máximoe**). Por padrão, o tempo de armazenamento dos objetos é de 90 dias e, depois disso, eles serão excluídos. Você pode alterar o tempo máximo de armazenamento ou até mesmo cancelar as restrições impostas.

- Especifique o tamanho máximo da área de armazenamento de dados (caixa ☑ **Tamanho máximo**). Por padrão, o tamanho máximo é 1000 MB. Você pode cancelar as restrições impostas para o tamanho do relatório ou inserir outro valor.

➡ Para configurar as definições de quarentena e backup:

1. Abra a janela de configuração do aplicativo.
2. À esquerda da janela, selecione a seção **Relatórios e Armazenamentos**.
3. Na seção **Quarentena e Backup**, marque as caixas desejadas e insira o tamanho máximo da área de armazenamento de dados, se necessário.

DISCO DE RECUPERAÇÃO

O Kaspersky Internet Security inclui um serviço que permite a criação de um disco de recuperação.

O Disco de recuperação é criado para verificar e desinfetar computadores infectados compatíveis com x86. Ele deve ser usado quando o nível de infecção não permite desinfetar o computador usando aplicativos antivírus ou utilitários de remoção de malware (como o Kaspersky AVPTool) executados no sistema operacional. Nesse caso, é obtido um nível de eficiência de desinfecção excepcionalmente alto, pois os programas de malware não tomam o controle enquanto o sistema operacional é carregado.

O Disco de recuperação é um arquivo .iso baseado no Linux que compreende:

- arquivos de sistemas e configurações de arquivos do Linux;
- um conjunto de utilitários de diagnóstico do sistema operacional;
- um conjunto de ferramentas adicionais (gerenciador de arquivos, etc.);
- arquivos do Disco de recuperação Kaspersky;
- arquivos que contêm bancos de dados de aplicativos.

Encerrando um computador com um sistema operacional corrompido pode ser feito de uma das duas seguintes maneiras:

- *localmente*, de um CD/DVD. Para fazê-lo, o computador deve ter o dispositivo adequado.
- *remotamente*, da estação de trabalho do administrador ou de outro computador na rede.

Remover a inicialização só é possível se um computador sendo encerrado suportar tecnologia de Administração Ativa Intel® vPro™ ou Intel®.

Para criar um Disco de recuperação, faça o seguinte:

1. Abra a janela principal do aplicativo.
2. Clique no botão **Disco de recuperação** para executar o Assistente Criação de Disco de Recuperação (veja página 89).
3. Siga as instruções do Assistente.
4. Crie um CD/DVD de inicialização usando o arquivo fornecido pelo assistente. Para fazê-lo, você pode usar qualquer aplicativo de gravação de CDs/DVDs, como o Nero.

CONSULTE TAMBÉM:

CRIANDO O DISCO DE RECUPERAÇÃO

Criar o disco de recuperação é o mesmo que criar uma imagem em disco (arquivo ISO) com arquivos de configuração e os bancos de dados de aplicativo atualizados.

A imagem do disco de origem que serve como base para a criação do novo arquivo pode ser baixada do servidor da Kaspersky Lab ou copiada de uma fonte local.

O arquivo de imagem criado pelo assistente será salvo na pasta "*Documents and Configurações\All Users\Application Data\Kaspersky Lab\AVP80\Data\Rdisk*" (ou "*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk*" – no Microsoft Vista) com o nome *rescuecd.iso*. Se o assistente detectar um arquivo ISSO criado anteriormente na pasta especificada, você poderá usá-lo como a imagem de disco original marcando a caixa ☑ **Usar arquivo de imagem existente** e passar para a Etapa 3 – atualizar imagem (veja página 90). Se o assistente não detectar um arquivo de imagem, esta caixa não estará disponível.

O Disco de Recuperação é criado com um assistente que consiste de uma série de caixas (passos). As caixas são navegadas com o **Voltar** e **Avançar**; o assistente termina essa atividade clicando no botão **Concluir**. Para interromper o assistente a qualquer etapa, use o botão **Cancelar**.

DISCUSSÃO DETALHADA DAS ETAPAS DO ASSISTENTE

ETAPA 1. SELECIONANDO A FONTE DE IMAGEM DO DISCO

Se você marcou a caixa ☑ **Usar arquivo ISO existente** na janela anterior do assistente, esta etapa será ignorada.

Nesta etapa, você deve selecionar a origem do arquivo da imagem na lista de opções:

- Selecione ◉ **Copiar a imagem ISO do CD/DVD ou da rede local** se já tiver um Disco de Recuperação em CD/DVD ou uma imagem preparada para ele armazenada no seu computador ou em um recurso da rede local.
- Selecione a opção ◉ **Baixar a imagem ISO do servidor da Kaspersky Lab** se não tiver nenhum arquivo de imagem existente; assim, você poderá baixá-lo do servidor da Kaspersky Lab (o tamanho do arquivo é aproximadamente 100 MB).

ETAPA 2. COPIANDO A IMAGEM ISO

Se, na etapa anterior, você selecionou a opção de copiar a imagem de uma fonte local (◉ **Copiar a imagem ISO do CD/DVD ou da rede local**), nesta etapa, você deve especificar o caminho da imagem. Para fazê-lo, use o botão **Procurar**. Em seguida, será exibido o andamento da cópia.

Se você selecionou ◉ **Baixar a imagem ISO do servidor da Kaspersky Lab**, o andamento do download do arquivo será exibido imediatamente.

ETAPA 3. ATUALIZAÇÃO DE IMAGEM ISO

O procedimento de atualização do arquivo inclui:

- atualização dos bancos de dados de aplicativos;
- atualização dos arquivos de configuração.

Arquivos de configuração determinam como o Disco de Recuperação deve ser usado: em um computador local ou em um computador remoto; log, você deve selecionar a opção antes de atualizar o arquivo ISO:

- ◉ **Inicialização remota** se carregar um computador remoto é a intenção.

  Note que se inicializar um computador remoto é selecionado, ele deve suportar a tecnologia de Administração Ativa Intel® vPro™ ou Intel®.

  Se o acesso à Internet de um computador remoto for garantido por um servidor proxy, então a atualização não estará disponível ao usar um Disco de Recuperação. Nesse caso, é recomendado atualizar de antemão o Kaspersky Anti-Virus.

- ◉ **Inicializar a partir de disco CD/DVD** se a intenção é que a imagem de disco sendo criada vá gravar em CD/DVD.

Tendo selecionado a opção desejada, clique no botão **Avançar**. O andamento da atualização será exibido na próxima janela do assistente.

Se você tiver selecionado a opção **Inicialização remota**, então a imagem criada não pode ser usada nem para gravar um CD/DVD, nem para carregar o computador. Para carregar o computador a partir de um CD/DVD, você deve executar o assistente novamente e selecionar a opção **Inicialização a partir de CD/DVD** nessa etapa.

ETAPA 4. INICIALIZAÇÃO REMOTA

Esta etapa do Assistente só aparece se você tiver selecionado a opção **Inicialização Remota** na etapa anterior.

Digite as informações sobre o computador:

- **Endereço de IP ou nome do computador** na rede;
- dados da conta do usuário com direitos de administrador de sistema: **Nome do usuário** e **Senha**.

A próxima janela do assistente é o console iAMT onde você pode controlar o processo de carregar o computador (veja página 91).

ETAPA 5. FECHANDO O ASSISTENTE

Esta janela do assistente informa que você criou um Disco de Recuperação com êxito.

INICIALIZANDO O COMPUTADOR USANDO O DISCO DE RECUPERAÇÃO

Se não for possível iniciar o sistema operacional devido a um ataque de vírus, use o Disco de Recuperação.

Você precisará do arquivo de imagem do disco de inicialização (.iso) para carregar o sistema operacional. Você pode baixar o arquivo (veja página 90) do servidor da Kaspersky Lab ou atualizar (veja página 90) o existente.

Vamos examinar mais detalhadamente o funcionamento do Disco de Recuperação. Ao carregar o disco, as seguintes operações são executadas:

1. Detecção automática do hardware do computador.
2. Pesquisa dos sistemas de arquivos nos discos rígidos. Serão atribuídos nomes iniciados com *C* aos sistemas de arquivos detectados.

   Os nomes atribuídos aos discos rígidos e aos dispositivos removíveis não podem corresponder aos nomes atribuídos a eles pelo sistema operacional.

   Se o sistema operacional do computador que está sendo carregado estiver no modo de suspensão ou se o status de seu sistema de arquivos for *com erros* devido a um desligamento incorreto, você poderá optar entre montar o sistema de arquivos ou reiniciar o computador.

   A montagem do sistema de arquivos pode resultar em sua corrupção.

3. Pesquisa do arquivo de permuta do Microsoft Windows *pagefile.sys*. Se ausente, o volume da memória virtual será limitado pelo tamanho da RAM.
4. Seleção do idioma do local. Se a seleção não for feita após um determinado tempo, o idioma inglês será definido por padrão.

   Ao carregar um computador remoto, esta etapa é omitida.

5. Pesquisa (criação) das pastas para os bancos de dados de antivírus, relatórios, armazenamento da Quarentena e arquivos adicionais. Por padrão, serão usadas as pastas dos aplicativos da Kaspersky Lab instalados no computador infectado (*ProgramData/Kaspersky Lab/AVP8* - no Microsoft Windows Vista, *Documents and Configurações/All Users/Application Data/Kaspersky Lab/AVP8* - em versões anteriores do

Microsoft Windows). Se não for possível encontrar essas pastas de aplicativos, será feita uma tentativa de criá-las. Se essas pastas não forem encontradas e não for possível criá-las, a pasta *kl.files* será criada em um disco do sistema.

6. Tentativa de configurar conexões de rede com base nos dados encontrados nos arquivos de sistema do computador que está sendo carregado.

7. Carregar um subsistema gráfico e inicializar o Disco de Recuperação do Kaspersky (ao carregar o computador de um CD/DVD).

   Se um computador remoto for carregado no console iAMT, o prompt de comando será carregado. Você pode usar os comandos para trabalhar com o Disco de Recuperação do Kaspersky a partir de uma linha de comando para gerenciar essas tarefas (veja página 92).

No modo de recuperação do sistema, apenas as tarefas de verificação de vírus e atualizações do banco de dados de uma fonte local estão disponíveis, além da reversão da atualização e da exibição de estatísticas.

➧ *Para carregar o sistema operacional de um computador infectado a partir de um CD/DVD, faça o seguinte:*

1. Nas configurações de BIOS, ative inicialização de CD/DVD-ROM (para informações detalhadas, consulte a documentação da placa mãe instalada no computador).

2. Insira o CD/DVD com a imagem do Disco de Recuperação na unidade de CD/DVD do computador infectado.

3. Reinicie o computador.

4. A inicialização continuará de acordo com o algoritmo descrito acima.

➧ *Para carregar o sistema operacional de um computador remoto, faça o seguinte:*

1. Abra a janela principal do aplicativo.

2. Clique no botão **Disco de recuperação** para executar o Assistente Criação de Disco de Recuperação (veja página 89). Siga as instruções do Assistente.

   Note que você deve selecionar a opção **Inicialização Remota** na etapa de atualização do disco (veja página 90).

A inicialização continuará de acordo com o algoritmo descrito acima.

TRABALHANDO COM O DISCO DE RECUPERAÇÃO DO KASPERSKY DO PROMPT DE COMANDO

Você pode trabalhar com o Disco de Recuperação do Kaspersky do prompt de comando. É possível executar as seguintes operações:

- verificar os objetos selecionados;
- atualizar os bancos de dados e módulos do aplicativo;
- revertendo a última atualização
- obter ajuda sobre a sintaxe da linha de comando;
- obter ajuda sobre a sintaxe de comandos.

Sintaxe de linha de comando:

```
<comando> [configurações]
```

O seguinte pode ser usado como comandos:

HELP	ajuda da sintaxe de comandos e lista de comandos.
SCAN	verifica objetos quanto a vírus
UPDATE	atualize a inicialização de tarefa
ROLLBACK	última atualização de rollback
EXIT	saia do Disco de Recuperação do Kaspersky

NESTA SEÇÃO

VERIFICAÇÃO DE VÍRUS

Para iniciar uma verificação de vírus em uma determinada área e processar objetos maliciosos no prompt de comando:

```
SCAN [<objeto verificado>] [<ação>] [<tipos de arquivos>] [<exclusões>]
[<configurações de relatório>]
```

Descrição das configurações:

<table>
<tr><td colspan="2"><objeto a ser verificado> – este parâmetro fornece a lista de objetos que serão verificados quanto à presença de código malicioso.

Ele pode incluir vários valores da lista fornecida separados por espaços.</td></tr>
<tr><td><arquivos></td><td>Lista de caminhos dos arquivos e/ou pastas a serem verificados.

Você pode inserir um caminho absoluto ou relativo para o arquivo. Os itens da lista são separados por um espaço.

Comentários:

• se o nome do objeto contiver um espaço, ele deve ser fornecido entre aspas;

• Se for feita uma referência a um diretório específico, todos os arquivos do diretório serão verificados.</td></tr>
<tr><td>/discos/</td><td>Verificando todas as unidades.</td></tr>
<tr><td>/discos/<nome_disco>:/<pasta></td><td>Verificando a unidade selecionada, onde o <nome_disco> é o nome da unidade, e <pasta> o caminho para a pasta sendo verificada.</td></tr>
<tr><td colspan="2"><ação> – este parâmetro determina que ações serão executadas com objetos maliciosos detectados durante a verificação. Se o parâmetro não for definido, a ação padrão será aquela com o valor para -i8.</td></tr>
<tr><td>-i0</td><td>Não é tomada nenhuma ação com relação ao objeto; suas informações são registradas no relatório.</td></tr>
</table>

-i1	Neutraliza objetos infectados e, se a desinfecção falhar, os ignora.
-i2	Neutraliza objetos infectados e, se a desinfecção falhar, os exclui. Não exclui objetos infectados de objetos compostos. Exclui objetos compostos infectados com cabeçalhos executáveis (arquivos comprimidos sfx) (esta é a configuração padrão).
-i3	Neutraliza objetos infectados e, se a desinfecção falhar, os exclui. Exclui completamente todos os objetos compostos, se não for possível excluir as partes infectadas.
-i4	Exclui os objetos infectados. Exclui completamente todos os objetos compostos, se não for possível excluir as partes infectadas.
-i8	Pergunta o que fazer se for detectado um objeto infectado.
-i9	Pergunta o que fazer no final da verificação.
<tipos de arquivos> – este parâmetro define os tipos de arquivos que serão verificados quanto à presença de vírus. Por padrão, se esse parâmetro não for definido, apenas os arquivos infectados de acordo com seu conteúdo serão verificados.	
-fe	Verifica somente os arquivos infectados de acordo com sua extensão.
-fi	Verifica somente os arquivos infectados de acordo com seu conteúdo.
-fa	Verifica todos os arquivos.
<exclusões> –este parâmetro define os objetos que serão excluídos da verificação. Ele pode incluir vários valores da lista fornecida separados por espaços.	
-e:a	Não verifica arquivos comprimidos.
-e:b	Não verifica bancos de dados de email.
-e:m	Não verifica emails em texto sem formatação.
-e:<máscara_arquivos>	Não verifica objetos que correspondem à máscara.
-e:<segundos>	Ignora objetos cujo tempo de verificação ultrapassa o tempo especificado no parâmetro **<segundos>**.
-es:<tamanho>	Ignora objetos cujo tamanho (em MB) excede o valor especificado no parâmetro **<tamanho>**.

Exemplos:

- *Inicie a verificação da pasta Documentos e Configurações e a unidade <D>:*

```
SCAN /discos/D: "/discos/C:/Documentos e Configurações "
```

ATUALIZAÇÃO DO KASPERSKY ANTI-VIRUS

O comando para atualizar os bancos de dados e módulos de programa do Kaspersky Anti-Virus possui a seguinte sintaxe:

```
UPDATE[<atualiza—fonte>][-R[A]:<arquivo_de_relatório>]
```

Descrição das configurações:

<fonte_de_atualização>	Servidor HTTP ou FTP ou pasta de rede para baixar as atualizações. O valor da configuração pode estar no formato de um caminho completo para uma fonte de atualização ou um URL. Se não for selecionado um caminho, a fonte da atualização será obtida das configurações de serviços de atualização.
-R[A]:<arquivo_de_relatório>	**-R:<arquivo_de_relatório> –** registra somente os eventos importantes no relatório. **-RA:<arquivo_de_relatório> –** registra todos os eventos no relatório. É permitido usar caminho absoluto para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Exemplos:

- *Atualizar os bancos de dados e registrar todos os eventos em um relatório:*

```
UPDATE -RA:/discos/C:/avbases_upd.txt
```

RETORNANDO A ÚLTIMA ATUALIZAÇÃO

Sintaxe do comando:

```
ROLBACK[-R[A]:<arquivo_de_relatório>
```

Descrição das configurações:

-R[A]:<arquivo_de_relatório>	**-R:<arquivo_de_relatório> –** registra somente os eventos importantes no relatório. **-RA:<arquivo_de_relatório> –** registra todos os eventos no relatório. É permitido usar caminho absoluto para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Exemplo:

```
ROLLBACK -RA:/discos/C:/rollback.txt
```

EXIBINDO A AJUDA

Use este comando para exibir a sintaxe da linha de comando do aplicativo:

```
[ -? | HELP ]
```

Para obter ajuda sobre a sintaxe de um comando específico, use um dos comandos a seguir:

```
<comando>-?
HELP <comando>
```

VALIDANDO AS CONFIGURAÇÕES DO KASPERSKY ANTI-VIRUS

Depois que o Kaspersky Anti-Virus for instalado e configurado, você poderá verificar se o aplicativo foi configurado corretamente, usando um "vírus" de teste e suas modificações. É necessário realizar um teste separado para cada componente / protocolo de proteção.

NESTA SEÇÃO

O "VÍRUS" DE TESTE DA EICAR E SUAS MODIFICAÇÕES

Este "vírus" de teste foi especialmente desenvolvido pelo eicar (The European Institute for Computer Antivirus Research) para testar produtos antivírus.

O "vírus" de teste NÃO É UM VÍRUS porque não contém nenhum código que possa danificar seu computador. Entretanto, a maioria dos produtos antivírus identifica esse arquivo como um vírus.

Nunca use vírus reais para testar o funcionamento de um produto antivírus!

Você pode baixar este "vírus" de teste no site oficial da **EICAR** em http://www.eicar.org/anti_virus_test_file.htm.

Antes de baixar o arquivo, desative a proteção antivírus do computador; caso contrário, o aplicativo identificará e processará o arquivo *anti_virus_test_file.htm* como um objeto infectado transferido através do protocolo HTTP. Não esqueça de ativar a proteção antivírus imediatamente depois de baixar o "vírus" de teste.

O aplicativo identifica o arquivo baixado do site da **EICAR** como um objeto infectado que contém um vírus que **não pode ser desinfetad**o e executa as ações especificadas para este tipo de objeto.

Também é possível modificar o "vírus" de teste padrão para verificar a operação do aplicativo. Para modificar o "vírus", altere o conteúdo do "vírus" padrão, adicionando um dos prefixos a ele (veja a tabela a seguir). Para modificar os "vírus" de teste, você pode usar qualquer editor de texto ou de hipertexto, como o **Bloco de Notas da Microsoft**, o **UltraEdit32**, etc.

É possível testar se a operação do aplicativo antivírus está correta usando o "vírus" da EICAR modificado somente se os seus bancos de dados de antivírus foram atualizados pela última vez em ou depois de 24 de outubro de 2003 (atualizações cumulativas de outubro de 2003).

A primeira coluna da tabela a seguir contém os prefixos que devem ser adicionados ao início da série do "vírus" de teste padrão. A segunda coluna lista todos os status possíveis que o aplicativo antivírus pode atribuir ao objeto com base nos resultados da verificação. A terceira coluna indica como o aplicativo processa os objetos com o status especificado. As ações reais executadas com os objetos são determinadas pelas configurações do aplicativo.

Depois de ter adicionado o prefixo ao "vírus" de teste, salve o novo arquivo com um nome diferente, por exemplo: *eicar_dele.com*. Atribua nomes semelhantes a todos os "vírus" modificados.

Table 1. Modificações do "vírus" de teste

Prefixo	Status do objeto	Informação sobre o processamento do objeto
Sem prefixo, "vírus" de teste padrão.	**Infectado**. O objeto contém o código de um vírus conhecido. Não é possível desinfetar o objeto.	O aplicativo identifica o objeto como um vírus que não pode se desinfetado. Ao tentar desinfetar o objeto, ocorre um erro; a ação executada será aquela especificada para objetos que não podem ser desinfetados.
CORR–	**Corrompido**.	O aplicativo pode acessar o objeto, mas não verificá-lo, pois ele está corrompido (por exemplo, a estrutura do arquivo está corrompida ou o formato do arquivo é inválido). Você pode encontrar informações de que o objeto foi processado no relatório de operação do aplicativo.
WARN–	**Suspeito**. O objeto contém o código de um vírus desconhecido. Não é possível desinfetar o objeto.	O objeto foi considerado suspeito pelo analisador de código heurístico. No momento da detecção, os bancos de dados de assinaturas de ameaças do antivírus não contêm uma descrição do procedimento para neutralizar esse objeto. Você será notificado quando um objeto desse tipo for detectado.
SUSP–	**Suspeito**. O objeto contém o código modificado de um vírus conhecido. Não é possível desinfetar o objeto.	O aplicativo detectou uma correspondência parcial de uma seção do código do objeto com uma seção do código de um vírus conhecido. No momento da detecção, os bancos de dados de assinaturas de ameaças do antivírus não contêm uma descrição do procedimento para neutralizar esse objeto. Você será notificado quando um objeto desse tipo for detectado.
ERRO–	**Erro de verificação**.	Ocorreu um erro durante a verificação de um objeto. O aplicativo não pode acessar o objeto, pois a integridade do mesmo foi violada (por exemplo, não existe um final em um arquivo comprimido com vários volumes) ou não é possível conectá-lo (se o objeto estiver sendo verificado em um recurso de rede). Você pode encontrar informações de que o objeto foi processado no relatório de operação do aplicativo.
CURE–	**Infectado**. O objeto contém o código de um vírus conhecido. Pode ser desinfetado.	O objeto contém um vírus que pode ser desinfetado. O aplicativo desinfetará o objeto; o texto do corpo do "vírus" será substituído pela palavra CURE. Você será notificado quando um objeto desse tipo for detectado.
DELE–	**Infectado**. O objeto contém o código de um vírus conhecido. Não é possível desinfetar o objeto.	O aplicativo identifica o objeto como um vírus que não pode se desinfetado. Ao tentar desinfetar o objeto, ocorre um erro; a ação executada será aquela especificada para objetos que não podem ser desinfetados. Você será notificado quando um objeto desse tipo for detectado.

VALIDANDO AS CONFIGURAÇÕES DO ANTIVÍRUS DE ARQUIVOS

Para verificar se a configuração do Antivírus de arquivos está correta:

1. Crie uma pasta em um disco, copie-o para vírus de teste baixado do site oficial da **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), e as modificações que você criou.
2. Todos os eventos devem ser registrados, de forma que o arquivo do relatório mantenha os dados de objetos corrompidos e objetos ignorados devido a erros.
3. Execute o "vírus" de teste ou alguma de suas versões modificadas.

O componente Antivírus de arquivos interceptará a chamada de execução do arquivo, o verificará e executará a ação especificada nas configurações para objetos com esse status. Ao selecionar ações diferentes a serem realizadas com o objeto detectado, você poderá executar uma verificação completa da operação do componente.

É possível exibir as informações sobre os resultados da operação do componente Antivírus de arquivos no relatório de operação do componente.

VALIDANDO AS CONFIGURAÇÕES DA TAREFA DE VERIFICAÇÃO DE VÍRUS

Para verificar se as configurações da tarefa de verificação de vírus estão corretas:

1. Crie uma pasta em um disco, copie-o para o "vírus" de teste baixado do site oficial da **EICAR** em (http://www.eicar.org/anti_virus_test_file.htm), e as modificações que você criou para ele.
2. Crie uma nova tarefa de verificação de vírus e selecione a pasta que contém o conjunto de "vírus" de teste como o objeto a ser verificado.
3. Todos os eventos devem ser registrados, de forma que o arquivo do relatório mantenha os dados de objetos corrompidos e objetos ignorados devido a erros.
4. Execute a tarefa de verificação de vírus.

Ao executar a tarefa de verificação, as ações especificadas nas configurações de tarefa serão realizadas conforme objetos suspeitos ou infectados sejam detectados. Ao selecionar ações diferentes a serem realizadas com o objeto detectado, você poderá executar uma verificação completa da operação do componente.

É possível exibir todas as informações sobre as ações da tarefa de verificação de vírus no relatório de operação do componente.

TIPOS DE NOTIFICAÇÕES

Quando ocorrem eventos de Anti-Vírus, são exibidas mensagens de notificação especiais. Dependendo do grau de importância do evento para a segurança do computador, você poderá receber os seguintes tipos de notificações:

- **Alarme**. Ocorreu um evento crítico; por exemplo, um objeto malicioso ou uma atividade perigosa foram detectados no sistema. Decida imediatamente como lidar com a ameaça. Este tipo de notificação está codificada pela cor vermelha.

- **Aviso**. Ocorreu um evento possivelmente perigoso. Por exemplo, foram detectados arquivos possivelmente infectados ou uma atividade suspeita no sistema. Você deverá decidir o nível de perigo que este evento representa. Este tipo de notificação está codificada pela cor amarela.

- **Informações**. Esta notificação fornece informações sobre eventos não-críticos. Notificações informativas são coloridas em código de azul.

NESTA SEÇÃO

OBJETO MALICIOSO DETECTADO

Se o Antivírus de arquivos ou uma verificação de vírus detectar um código malicioso, será exibida uma notificação pop-up especial.

A notificação contém:

- O tipo de ameaça (por exemplo, *vírus*, *cavalo de Troia*) e o nome do objeto malicioso, conforme listado na Enciclopédia de vírus da Kaspersky Lab. O nome do objeto perigoso é fornecido como um link para www.viruslist.com, onde você pode encontrar informações mais detalhadas sobre o tipo de ameaça detectada no computador.

- O nome completo do objeto malicioso e o caminho para ele.

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Desinfetar** – tenta desinfetar o objeto malicioso. Antes do tratamento, é criada uma cópia de backup do objeto, caso seja necessário restaurá-lo ou ter uma imagem da infecção.

- **Excluir** – exclui o objeto malicioso. Antes de excluir, é criada uma cópia de backup do objeto, caso seja necessário restaurá-lo ou ter uma imagem da infecção.

- **Ignorar** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Posteriormente, você pode voltar aos objetos maliciosos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual do componente de proteção ou de uma operação da tarefa, marque a caixa ☑ **Aplicar a todos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o aplicativo ser reiniciado, ou o período entre o início e a conclusão de uma tarefa de verificação de vírus.

O OBJETO NÃO PODE SER DESINFETADO

Às vezes, não é possível desinfetar um objeto malicioso. Isso pode acontecer quando um arquivo está tão danificado que é impossível excluir o código malicioso e restaurar sua integridade. O procedimento de neutralização não pode ser aplicado a diversos tipos de objetos perigosos, como os cavalos de Troia.

Nesses casos, uma notificação pop-up especial será exibida, contendo:

- O tipo de ameaça (por exemplo, *vírus*, *cavalo de Troia*) e o nome do objeto malicioso, conforme listado na Enciclopédia de vírus da Kaspersky Lab. O nome do objeto perigoso é fornecido como um link para www.viruslist.com, onde você pode encontrar informações mais detalhadas sobre o tipo de ameaça detectada no computador.
- O nome completo do objeto malicioso e o caminho para ele.

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Excluir** – exclui o objeto malicioso. Antes de excluir, é criada uma cópia de backup do objeto, caso seja necessário restaurá-lo ou ter uma imagem da infecção.
- **Ignorar** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Posteriormente, você pode voltar aos objetos maliciosos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual do componente de proteção ou a tarefa, marque a caixa ☑ **Aplicar a todos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o aplicativo ser reiniciado, ou o período entre o início e a conclusão de uma tarefa de verificação de vírus.

OBJETO SUSPEITO DETECTADO

Se o Antivírus de arquivos ou uma verificação de vírus detectar um objeto que contém o código de um vírus desconhecido ou o código modificado de um vírus conhecido, será exibida uma notificação pop-up especial.

A notificação contém:

- O tipo de ameaça (por exemplo, *vírus*, *cavalo de Troia*) e o nome do objeto, conforme listado na Enciclopédia de vírus da Kaspersky Lab. O nome do objeto perigoso é fornecido como um link para www.viruslist.com, onde você pode encontrar informações mais detalhadas sobre o tipo de ameaça detectada no computador.
- O nome completo do objeto e o caminho para ele.

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Quarentena** – colocar o objeto em quarentena. Quando um objeto é colocado na Quarentena, ele é movido e não copiado: o objeto é excluído do disco ou do email e salvo na pasta Quarentena. Os arquivos na Quarentena são salvos em um formato especial e não são perigosos.

  Mais tarde, ao verificar a Quarentena com assinaturas de ameaças atualizadas, o status do objeto poderá mudar. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status de não *infectado* e ele pode ser restaurado.
- **Excluir** - exclui o objeto. Antes de excluir, é criada uma cópia de backup do objeto, caso seja necessário restaurá-lo ou ter uma imagem da infecção.
- **Ignorar** – bloquear o acesso ao objeto, mas não executar qualquer ação com ele; simplesmente registrar suas informações em um relatório.

Posteriormente, você pode voltar aos objetos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual do componente de proteção ou de uma operação da tarefa, marque a caixa ☑ **Aplicar a todos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o aplicativo ser reiniciado, ou o período entre o início e a conclusão de uma tarefa de verificação de vírus.

Se tiver certeza de que o objeto detectado não é malicioso, é recomendável adicioná-lo à zona confiável para evitar que o aplicativo repita falsos positivos quando você usar o objeto.

TRABALHANDO COM O APLICATIVO NA LINHA DE COMANDO

Você pode trabalhar com o Kaspersky Anti-Virus na linha de comando.

Sintaxe de linha de comando:

```
avp.com <comando> [opções]
```

Acesse o aplicativo da linha de comando a partir da pasta de instalação do Kaspersky Anti-Virus ou especificando o caminho completo para avp.com.

Os comandos a seguir podem ser usados como <comando>:

- **HELP –** ajuda da sintaxe de comandos e lista de comandos.
- **SCAN –** verifica os objetos para detectar malware.
- **UPDATE –** inicia a atualização do aplicativo.
- **ROLLBACK –** reverte para a última atualização do Kaspersky Anti-Virus (o comando só pode ser executado se a senha atribuída por meio da interface do aplicativo for digitada).
- **START –** inicia um componente ou uma tarefa.
- **STOP –** interrompe um componente ou uma tarefa (o comando só pode ser executado se a senha atribuída por meio da interface do Kaspersky Anti-Virus for digitada).
- **STATUS –** exibe o status atual do componente ou da tarefa na tela.
- **STATISTICS –** exibe o status atual do componente ou da tarefa na tela.
- **EXPORT –** exporta as configurações de proteção do aplicativo.
- **IMPORT –** importa as configurações de proteção do aplicativo (o comando só pode ser executado se a senha atribuída por meio da interface do Kaspersky Anti-Virus for inserida).
- **ACTIVATE –** ativa o Kaspersky Anti-Virus via Internet usando um código de ativação.
- **ADDKEY –** ativa o aplicativo usando um arquivo chave (o comando só poderá ser executado se a senha atribuída por meio da interface do aplicativo for digitada).
- **RESTORE –** restaura um arquivo de quarentena.
- **EXIT –** encerra o aplicativo usando um arquivo chave (o comando só poderá ser executado se a senha atribuída por meio da interface do aplicativo for digitada).
- **TRACE –** obtém um arquivo de rastreamento.

Cada comando exige seu próprio conjunto específico de parâmetros.

NESTA SEÇÃO

EXIBINDO A AJUDA

Use este comando para exibir a sintaxe da linha de comando do aplicativo:

```
avp.com [ /? | HELP ]
```

Para obter ajuda sobre a sintaxe de um comando específico, use um dos comandos a seguir:

```
avp.com <comando> /?
avp.com HELP <comando>
```

VERIFICAÇÃO DE VÍRUS

Para iniciar uma verificação de vírus em uma determinada área e processar objetos maliciosos no prompt de comando:

```
avp.com SCAN [<objeto verificado>] [<ação>] [<tipos de arquivos>] [<exclusões>]
[<configurações relatório>] [<configurações avançadas>]
```

Para verificar objetos, você também pode usar as tarefas criadas no aplicativo, iniciando-as na linha de comando. A tarefa será executada com as configurações especificadas na interface do Kaspersky Anti-Virus.

Descrição das configurações:

<objeto a ser verificado> – este parâmetro fornece a lista de objetos que serão verificados quanto à presença de código malicioso. Ele pode incluir diversos valores da lista fornecida separados por espaços:

- **<arquivos>** – lista de caminhos para os arquivos e / ou pastas a serem verificadas. Você pode inserir um caminho absoluto ou relativo para o arquivo. Os itens da lista são separados por um espaço. Comentários:

- Se o nome do objeto contiver um espaço, ele deve ser colocado entre aspas;
  - Se for feita uma referência a uma pasta específica, todos os arquivos dessa pasta serão verificados.

- **/ALL** – verificação completa do computador.
- **/MEMORY** – objetos de RAM.
- **/STARTUP** – objetos de inicialização.
- **/MAIL** – bancos de dados de mensagens.
- **/REMDRIVES** – todas as unidades removíveis.
- **/FIXDRIVES** – todas as unidades locais.
- **/NETDRIVES** – todas as unidades de rede.
- **/QUARANTINE** – objetos em quarentena.
- **/@:<filelist.lst>** – caminho para um arquivo que contém uma lista de objetos e catálogos a serem verificados. O arquivo deve estar no formato de texto e cada objeto da verificação deve estar listado em uma linha separada. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se contiver espaços, o caminho deve ser colocado entre aspas.

<ação> – este parâmetro determina que ações serão executadas com objetos maliciosos detectados durante a verificação. Se este parâmetro não for definido, a ação padrão será aquela com o valor para **/i2**. Os seguintes valores são possíveis:

- **/i0** – não efetuar nenhuma ação com relação ao objeto; simplesmente registrar suas informações no relatório.
- **/i1** – neutralizar objetos infectados e, se a desinfecção for impossível, ignorá-los.
- **/i2** – neutralizar objetos infectados e se a desinfecção falhar, exclui-los. Não exclui objetos infectados de objetos compostos. Exclui objetos compostos infectados com cabeçalhos executáveis (arquivos comprimidos sfx). Esta é a configuração padrão.
- **/i3** – neutralizar objetos infectados e se a desinfecção falhar, exclui-los. Exclui completamente todos os objetos compostos, se não for possível excluir as partes infectadas.
- **/i4** – excluir objetos infectados. Exclui completamente todos os objetos compostos, se não for possível excluir as partes infectadas.
- **/i8** – Pergunta o que fazer se for detectado um objeto infectado.
- **/i9** – Pergunta o que fazer no final da verificação.

<tipos de arquivos> – este parâmetro define os tipos de arquivos que serão verificados quanto à presença de vírus. Por padrão, se esse parâmetro não for definido, apenas os arquivos infectados de acordo com seu conteúdo serão verificados. Os seguintes valores são possíveis:

- **/fe** – verificar somente os arquivos infectados de acordo com sua extensão.
- **/fi** – verificar somente os arquivos infectados de acordo com seu conteúdo.
- **/fa** – verificar todos os arquivos.

<exclusões> –este parâmetro define os objetos que serão excluídos da verificação. Ele pode incluir vários valores da lista fornecida separados por espaços.

- **/e:a** – não verificar arquivos comprimidos.

- **/e:b** – não verificar bancos de dados de email.
- **/e:m** – não verificar emails em texto sem formatação.
- **/e:<máscara>** – não verificar objetos que correspondam à máscara.
- **/e:<segundos>** – ignorar objetos cujo tempo de verificação ultrapassa o tempo especificado no parâmetro **<segundos>**.

<configurações relatório> – este parâmetro determina o formato do relatório de resultados da verificação. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

- **/R:<arquivo_relatório>** – registra somente os eventos importantes nesse arquivo.
- **/RA:<arquivo_relatório>** – registra todos os eventos neste arquivo.

<configurações avançadas> – configurações que definem o uso das tecnologias de verificação antivírus e do arquivo de configuração para as configurações:

- **/iChecker=<on|off>** – ativar / desativar o uso da tecnologia iChecker.
- **/iSwift=<on|off>** – ativar / desativar o uso da tecnologia iSwift.
- **\/C:<nome do_arquivo_de configuração>** – define o caminho do arquivo de configuração que contém as configurações do aplicativo para a verificação. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores definidos na interface do aplicativo.

Exemplos:

- *Iniciar a verificação da memória, dos objetos de inicialização, dos bancos de dados de correio, dos diretórios Meus documentos e Arquivos de programas e do arquivo test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL C:\Documentos and Configurações\All Users\Meus
documentos" "C:\Arquivos de programas" "C:\Downloads\test.exe"
```

- *Verificar os objetos listados no arquivo object2scan.txt. usando o arquivo de configuração scan_setting.txt para o trabalho. Usar o arquivo de configuração scan_setting.txt. Ao concluir a verificação, criar um relatório de todos os eventos:*

```
avp.com SCAN/MEMORY /@:objects2scan.txt /C:scan_Configurações.txt /RA:scan.log
```

Um exemplo de arquivo de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_Configurações.txt /RA:scan.log
```

ATUALIZANDO O APLICATIVO

A sintaxe para atualizar os módulos do Kaspersky Anti-Virus e os bancos de dados do aplicativo da linha de comando é a seguinte:

```
avp.com UPDATE [<atualizar_fonte>] [/APP=<on|off>] [<configurações_relatório>]
[<configurações_avançadas>]
```

Descrição das configurações:

<atualizar_fonte> – Servidor HTTP ou FTP ou pasta de rede para baixar as atualizações. Se não for selecionado um caminho, a fonte da atualização será obtida da configurações de atualização do aplicativo.

/APP=<on|off> – ativa / desativa as atualizações dos módulos do aplicativo.

<configurações relatório> – este parâmetro determina o formato do relatório de resultados da verificação. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados. Os seguintes valores são possíveis:

- **/R:<arquivo_relatório>** – registra somente os eventos importantes nesse arquivo.
- **/RA:<arquivo_relatório>** – registra todos os eventos neste arquivo.

<configurações avançadas> – configurações que definem o uso do arquivo de configuração para as configurações.

\/C:<nome do_arquivo_de configuração> – define o caminho do arquivo de configuração que contém as configurações do aplicativo para a verificação. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores definidos na interface do aplicativo.

Exemplos:

- *Atualizar os bancos de dados do aplicativo e registrar todos os eventos no relatório:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Atualizar os módulos do programa Kaspersky Anti-Virus usando os parâmetros do arquivo de configuração updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

RETORNANDO A ÚLTIMA ATUALIZAÇÃO

Sintaxe do comando:

```
avp.com ROLLBACK </senha=<senha>> [<configurações_do relatório>]
```

Descrição das configurações:

</senha=<senha>> – a senha atribuída por meio da interface do aplicativo. O comando ROLLBACK não será executado sem inserir a senha.

<configurações de relatório> – configurações que definem o formato do relatório de resultados da verificação. É possível usar um caminho absoluto e relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

- **/R:<arquivo_relatório>** – registra somente os eventos importantes nesse arquivo.
- **/RA:<arquivo_relatório>** – registra todos os eventos neste arquivo. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Exemplo:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

INICIANDO/INTERROMPENDO A OPERAÇÃO DO ANTIVÍRUS DE ARQUIVOS OU UMA TAREFA

A sintaxe do comando START:

```
avp.com START <perfil|nome_tarefa> [configurações_relatório>]
```

A sintaxe do comando STOP:

```
avp.com STOP <perfil|nome_tarefa> </senha=<senha>>
```

Descrição das configurações:

</senha=<senha>> – a senha atribuída por meio da interface do aplicativo. O comando STOP não será executado sem inserir a senha.

<configurações relatório> – este parâmetro determina o formato do relatório de resultados da verificação. É possível usar um caminho absoluto e relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados. Os seguintes valores são possíveis:

- **/R:<arquivo_relatório>** – registra somente os eventos importantes nesse arquivo.
- **/RA:<arquivo_relatório>** – registra todos os eventos neste arquivo. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

A configuração **<perfil|tarefa_nome>** pode ter um dos seguintes valores:

- **Proteção (RTP)** – todos os componentes de proteção;
- **File_Monitoring (FM)** – Antivírus de arquivos;
- **Scan_My_Computer** – verificação completa do computador;
- **Scan_Objects** – verificação de objetos;
- **Scan_Quarantine** – verificação de quarentena;
- **Scan_Startup (STARTUP)** – verificação de objetos de inicialização;
- **Updater** – tarefa de atualização;
- **Rollback** – atualiza as tarefas de reversão.

Os componentes e tarefas iniciados na linha de comando são executados com as configurações definidas na interface do aplicativo.

Exemplos:

Para ativar o Antivírus de arquivos, digite no prompt de comando:

```
avp.com START FM
```

Para interromper a tarefa de verificação completa, insira:

avp.com STOP SCAN_MY_COMPUTER /password=<sua_senha>

ESTATÍSTICAS DA OPERAÇÃO DE UM COMPONENTE OU DE UMA TAREFA

A sintaxe do comando STATUS:

```
avp.com STATUS <perfil|nome_tarefa>
```

A sintaxe do comando STATISTICS:

```
avp.com STATUS <perfil|nome_tarefa>
```

Descrição das configurações:

A configuração **<perfil|nome_tarefa>** pode ter um dos valores especificados no comando START / STOP (ver página 106).

EXPORTANDO AS CONFIGURAÇÕES DE PROTEÇÃO

Sintaxe do comando:

```
avp.com EXPORT <perfil|nome_tarefa> <nome_arquivo>
```

Descrição das configurações:

A configuração **<perfil|nome_tarefa>** pode ter um dos valores especificados no comando START / STOP(veja página 106).

<nome_arquivo> – caminho do arquivo para o qual as configurações do aplicativo estão sendo exportadas. É possível especificar um caminho absoluto ou relativo.

Exemplo:

```
avp.com EXPORT RTP RTP_settings.dat - formato binário
avp.com EXPORT FM FM_settings.txt - formato de texto
```

IMPORTANDO AS CONFIGURAÇÕES DE PROTEÇÃO

Sintaxe do comando:

```
avp.com IMPORT <nome_arquivo> </senha=<sua_senha>>
```

Descrição das configurações:

<nome_arquivo> – caminho do arquivo do qual as configurações do aplicativo estão sendo importadas. É possível especificar um caminho absoluto ou relativo.

</senha=<sua_senha>> – uma senha atribuída por meio da interface do aplicativo.

Exemplo:

```
avp.com IMPORT settings.dat
```

ATIVANDO O APLICATIVO

Você pode ativar o Kaspersky Anti-Virus de duas maneiras:

- pela Internet, usando um código de ativação (comando ACTIVATE);
- usando um arquivo de chave (comando ADDKEY).

Sintaxe do comando:

```
avp.com ACTIVATE <código_ativação> </senha=<senha>>
avp.com ADDKEY <nome_arquivo> </senha=<senha>>
```

Descrição das configurações:

<código_ativação> – o código de ativação: xxxxx-xxxxx-xxxxx-xxxxx.

<nome_arquivo> – nome do arquivo de chave do aplicativo com a extensão .key: xxxxxxxx.key.

</senha=<senha>> – a senha atribuída por meio da interface do aplicativo.

Exemplo:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </senha=<senha>>
```

RESTAURANDO UM ARQUIVO DA QUARENTENA

Sintaxe do comando:

```
avp.com RESTORE [/REPLACE] <nome_arquivo>
```

Descrição das configurações:

/REPLACE – substituição do arquivo existente.

<nome_arquivo> – o nome do arquivo para restaurar.

Exemplo:

```
avp.com REPLACE C:\eicar.com
```

ENCERRAMENTO DO APLICATIVO

Sintaxe do comando:

```
avp.com EXIT </senha=<senha>>
```

Descrição das configurações:

</senha=<senha>> – a senha atribuída por meio da interface do aplicativo. O comando não será executado sem inserir a senha.

OBTENDO UM ARQUIVO DE RASTREAMENTO

Talvez seja necessário criar um arquivo de rastreamento, caso você tenha problemas com o Kaspersky Anti-Virus. Os arquivos de rastreamento são úteis para solucionar problemas e são usados extensivamente pelos especialistas do Suporte técnico.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off] [<nível_de_rastreamento>]
```

Descrição das configurações:

[on|off] – ativa / desativa a criação do arquivo de rastreamento.

[arquivo] – saída do rastreamento em arquivo.

<nível_de rastreamento> – Este valor pode ser um número inteiro, de 100 (nível mínimo, apenas mensagens críticas) a 600 (nível máximo, todas as mensagens).

Quando contatar o Serviço de suporte técnico, especifique o nível de rastreamento requerido. Se o nível não for especificado, é recomendável configurá-lo como 500.

Exemplos:

➧ *Para desativar a criação do arquivo de rastreamento:*

```
avp.com TRACE file off
```

➧ *Criar um arquivo de rastreamento com o nível de rastreamento de 500:*

```
avp.com TRACE file on 500
```

CÓDIGOS DE RETORNO DA LINHA DE COMANDO

Os códigos gerais podem ser retornados por qualquer comando da linha de comando. Os códigos de retorno incluem códigos gerais e códigos específicos de um determinado tipo de tarefa.

Códigos de retorno gerais:

- 0 – Operação concluída com êxito;
- 1 – Valor de configuração inválido;
- 2 – Erro desconhecido;
- 3 – Erro ao concluir a tarefa;
- 4 – Tarefa cancelada.

Códigos de retorno da tarefa de verificação de vírus:

- 101 – Todos os objetos perigosos foram processados;
- 102 – Objetos perigosos detectados.

MODIFICANDO, CONSERTANDO OU REMOVENDO O APLICATIVO

Você pode desinstalar o aplicativo das seguintes maneiras:

- usando o assistente de configuração do aplicativo;
- do prompt de comando (veja a seção "Desinstalando o aplicativo do prompt de comando" na página 112);
- usando o Kit de Administração Kaspersky (consulte Guia de Implementação do Kit de Administração Kaspersky);
- usando as políticas de grupo de domínio do Microsoft Windows Server 2000/2003 (consulte a seção "Desinstalando o aplicativo " na página 22).

NESTA SEÇÃO

MODIFICANDO, CONSERTANDO E REMOVENDO O APLICATIVO USANDO O ASSISTENTE DE INSTALAÇÃO

Você poder achar necessário consertar o aplicativo se detectou erros de operação depois de uma configuração incorreta ou corrupção de arquivo.

Para consertar ou modificar os componentes do Kaspersky Anti-Virus ou desinstalar o aplicativo:

1. Insira o CD de instalação na unidade de CD\DVD-ROMse você usou um para instalar o aplicativo. Se você instalou o Kaspersky Anti-Virus de uma fonte diferente (pasta de acesso público, pasta no seu disco rígido, etc.), verifique se o pacote do aplicativo está no local fornecido e se você tem acesso ao mesmo.
2. Selecione **Start** → **Programs** → **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** → **Modificar, Consertar ou Remover**.

O assistente de instalação abrirá então para o programa. Vamos examinar mais de perto as etapas de conserto, modificação, ou remoção do aplicativo.

ETAPA 1. JANELA BEM-VINDO À INSTALAÇÃO

Se você seguiu todas as etapas descritas acima e precisa consertar ou modificar o aplicativo, a janela bem-vindo à instalação do Kaspersky aparecerá. Clique no botão **Avançar** para continuar.

ETAPA 2. SELECIONANDO UMA OPERAÇÃO

Nessa etapa, você deve selecionar que operação deseja executar no aplicativo. Você pode modificar os componentes do aplicativo, consertar os componentes já instalados, ou remover vários componentes ou todo o aplicativo. Para executar a operação que você precisa, clique no botão apropriado. A resposta do programa de instalação depende da operação que você selecionou.

Modificar o aplicativo é similar à instalação de aplicativo personalizado onde você pode especificar quais componentes deseja instalar, e quais deseja excluir.

Consertar o aplicativo depende dos componentes instalados do aplicativo. Os arquivos serão consertados para todos os componentes que você instalou e o Nível de segurança **Recomendado** será definido para cada um deles.

Quando o Kaspersky Anti-Virus 6.0 for desinstalado remotamente, o servidor não será reiniciado automaticamente. Porém, para excluir os componentes do aplicativo e garantir um funcionamento correto do computador no futuro, é recomendável reiniciar o servidor manualmente.

Ao remover o aplicativo, você pode selecionar quais dados criados e usados pelo aplicativo você deseja salvar no computador. Para excluir os dados do Kaspersky Anti-Virus, selecione a opção **Desinstalação completa**. Para salvar dados, selecione a opção **Salvar objetos do aplicativo** e especifique quais objetos não devem ser excluídos:

- *Informações de ativação* – o arquivo de chave necessário para trabalhar com o aplicativo.
- *Bancos de dados do aplicativo* – conjunto completo de assinaturas de programas, vírus e outras ameaças perigosas, atuais desde a última atualização.
- *Backup de objetos* - backup de cópias de objetos excluídos ou desinfetados. Recomendamos que salve esses objetos, para que possam ser recuperados mais tarde.
- *Objetos em quarentena* - objetos que são potencialmente infectados por virus ou suas modificações. Esses objetos contêm um código similar ao código de um vírus conhecido mas é difícil determinar se são maliciosos. É recomendável salvá-los, já que eles podem ser inofensivos ou poderiam ser desinfetados depois de atualizar as assinaturas de ameaça.
- *Configurações de proteção* – valores para as configurações de todos os componentes do aplicativo.
- *Dados iSwift* - banco de dados com informações sobre objetos verificados no NTFS. Isso permite aumentar a velocidade de verificação. Usando este banco de dados, o Kaspersky Anti-Virus só verifica os arquivos que foram modificados desde a última verificação.

Se um período longo passar entre a desinstalação de uma versão do Kaspersky Anti-Virus e a instalação de uma outra, recomendamos que usem o banco de dados do iSwift salvo de uma instalação anterior do aplicativo. Um programa malicioso pode penetrar no computador durante esse período e seus efeitos não poderiam ser detectados pelo banco de dados, o que poderia levar a uma infecção.

Para iniciar a operação selecionada, clique no botão **Avançar**. O aplicativo começará a copiar os arquivos necessários para o computador ou excluir os componentes e dados selecionados.

ETAPA 3. CONCLUINDO A MODIFICAÇÃO, CONSERTO OU REMOÇÃO DO APLICATIVO

O processo de modificação, conserto ou remoção é exibido na tela, e após isso você será informado sobre a sua finalização.

Remover o programa geralmente requer que você reinicialize o computador depois, já que é necessário dar conta das modificações feitas no seu sistema. O aplicativo perguntará se você deseja reiniciar o computador. Clique no botão **Sim** e reinicie imediatamente. Para reiniciar o seu computador mais tarde, clique no botão **Não**.

REMOVENDO O APLICATIVO DO PROMPT DE COMANDO

➡ *Para desinstalar o Kaspersky Anti-Virus 6.0 para Windows Servers MP4 do prompt de comando, execute o seguinte:*

```
msiexec /x <nome do pacote>
```

O assistente de instalação abrirá. Você pode usá-lo para desinstalar o aplicativo.

- *Para desinstalar o aplicativo no modo não-interativo sem reiniciar o computador (o computador deve ser reiniciado após a desinstalação), insira o seguinte:*

```
msiexec /x <nome_do_pacote>/qn
```

- *Para desinstalar o aplicativo no modo não-interativo e então reiniciar o computador, insira o seguinte:*

```
msiexec /x <nome_do_pacote>ALLOWREBOOT=1/qn
```

Se você escolheu proteção de senha contra a desinstalação do computador quando instalou o aplicativo, será preciso você confirmar a senha ao desinstalar o aplicativo. De outro modo, o aplicativo não poderá ser desinstalado.

- *Para remover o aplicativo protegido por senha, insira o seguinte:*

`msiexec /x <nome_do_pacote > KLUNINSTPASSWD=******` – para remover o aplicativo no modo interativo.

`msiexec /x <nome_do_pacote > KLUNINSTPASSWD=****** /qn` – para remover o aplicativo no modo não-interativo.

GERENCIAR O APLICATIVO ATRAVÉS DO KIT DE ADMINISTRAÇÃO KASPERSKY

O **Kit de Administração Kaspersky** é um sistema de gerenciamento central de tarefas administrativas chave na operação de um sistema de segurança para uma rede corporativa, baseada em aplicativos incluídos no Kaspersky Anti-Virus Open Space Security. O Kit de Administração Kaspersky suporta todas as configurações de rede que usam TCP/IP.

O aplicativo é para administradores e redes corporativas de computadores e funcionários responsáveis pela proteção anti-vírus em suas empresas.

O Kaspersky Anti-Virus 6.0 para Windows Servers MP4 é um dos produtos da Kaspersky Lab que podem ser administrados através da própria interface de aplicativos, o prompt de comando (esses métodos estão descritos acima), ou usando o programa Kit de Administração Kaspersky (se o computador fizer parte de um sistema de administração remoto centralizado).

Para administrar o Kaspersky Anti-Virus através do Kit de Administração Kaspersky:

- implemente o *Servidor de Administração* na rede;
- instale o *Console de Administração* na estação de trabalho do administrador (para maiores detalhes consulte o Guia de Instalação do Kit de Administração Kaspersky);
- Instale o Kaspersky Anti-Virus e o *Network Agent* (incluídos no Kit de Administração Kaspersky) nos computadores em rede. Para maiores detalhes sobre a instalação remota do pacote de instalação do Kaspersky Anti-Virus em computadores em rede, consulte o Guia de Instalação do Kit de Administração Kaspersky.

> Antes de atualizar o plug-in do Kaspersky Anti-Virus através do Kit de Administração Kaspersky, encerre o Console de Administração.

O Console de Administração (consulte a figura abaixo) permite que você administre o aplicativo através do Kaspersky Administration Kit. Fornece uma interface integrada MMC padrão e permite ao administrador executar as seguintes funções:

- instalar e desinstalar remotamente o Kaspersky Anti-Virus e o *Network Agent* em computadores em rede;
- configurar remotamente o Kaspersky Anti-Virus em computadores em rede;
- atualizar os bancos de dados e módulos do Kaspersky;
- gerenciar licenças para o Kaspersky Anti-Virus em computadores em rede;
- exibir informações sobre a operação do aplicativo em computadores de clientes.
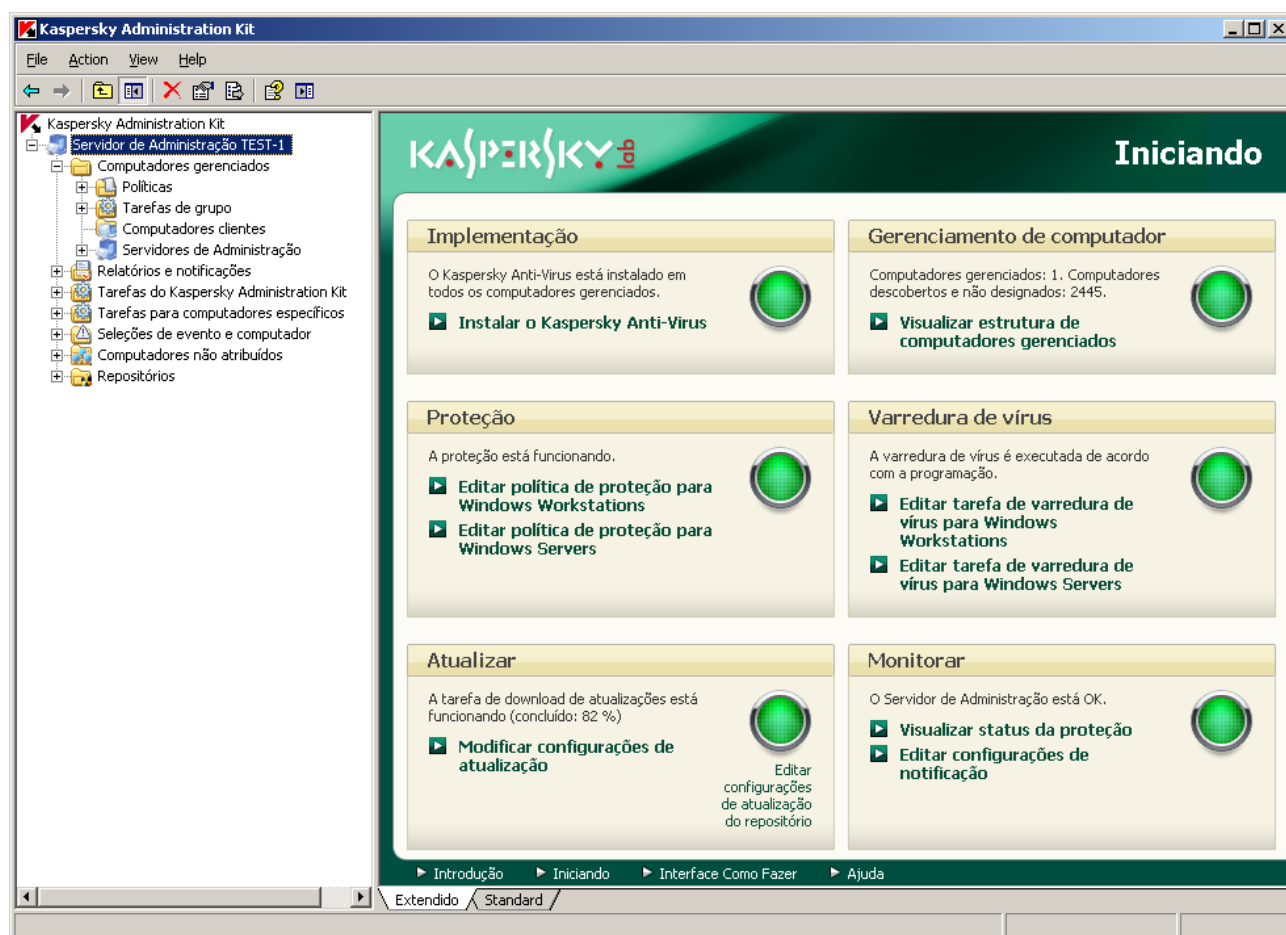
Figura 11. Console de Administração do Kaspersky Administration Kit

A aparência da janela do Kaspersky Administration Kit pode variar dependendo do sistema operacional do computador que você estiver usando.

Ao trabalhar com o Kaspersky Administration Kit, o aplicativo é gerenciado por configurações de política, configurações de tarefa, e configurações de aplicativos, definidos pelo administrador.

Medidas designadas tomadas pelo *aplicativo* são chamadas tarefas. Com base nas funções que desempenham, as tarefas se dividem em *tipos*: tarefas de verificação de vírus, tarefas de atualização de aplicativos, reversões de atualização, e tarefas de instalação de arquivo de chave.

Cada tarefa possui uma coleção de configurações para o aplicativo que são usadas quando ele é executado. As configurações de tarefas para o aplicativo são comuns para todos os tipos de *configurações de aplicativo*. As configurações de aplicativos que são específicas de um tipo de tarefas formam *configurações de tarefas*. As configurações de aplicativo e as configurações de tarefa não se sobrepõem.

O recurso chave da administração centralizada é agrupar computadores remotos em rede e gerenciá-los criando políticas de grupo de configuração.

A política é uma coleção de configurações de aplicativo para um grupo, bem como uma coleção de restrições sobre a re-edição dessas configurações ao configurar o aplicativo ou tarefas no computador de um cliente em particular. Uma política inclui definições para configurar todos os recursos do aplicativo, com a exceção de definições personalizadas para instâncias específicas de uma tarefa. Por exemplo, programar configurações.

Logo, políticas incluem as seguintes configurações:

- Configurações comuns a todas as tarefas (configurações de aplicativo);
- Configurações comuns a todas as instâncias de um tipo único de tarefa (principalmente configurações de tarefa).

Isso significa que uma política para o Kaspersky Anti-Virus, as tarefas que incluem proteção contra vírus e tarefas de verificação, incluem todas as configurações necessárias para configurar um aplicativo ao executar ambos os tipos de tarefas, mas não, por exemplo, uma programação para executar as tarefas ou configurações que definem o escopo da verificação.

NESTA SEÇÃO

GERENCIANDO O APLICATIVO

O Kaspersky Administration Kit dá a você a oportunidade de iniciar remotamente e interromper o Kaspersky Anti-Virus em computadores de clientes individuais, bem como de modificar as configurações gerais para o aplicativo, tal como ativar/desativar a proteção de computadores, modificando as configurações para Backup e Quarentena e prestação de relatórios.
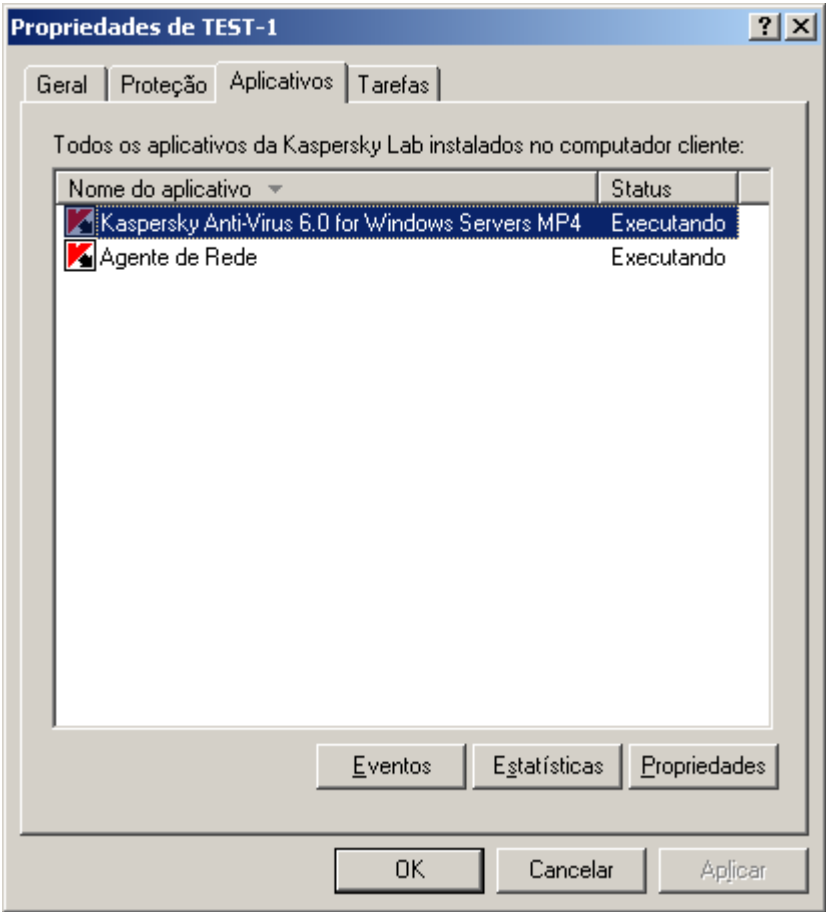
*Figura 12. Janela de propriedades do computador do cliente. A aba **Aplicativos***

Para Gerenciar o as configurações do aplicativo, faça o seguinte:

1. Abra o Kaspersky Administration Kit.
2. Selecionar a pasta **Computadores gerenciados** com o nome do grupo que inclui o computador do cliente.
3. No grupo selecionado, abrir a pasta **Computadores de clientes** e selecionar o computador no qual você precisa modificar as configurações do aplicativo.
4. Selecionar o comando **Propriedades** do menu contexto ou o item correspondente do menu **Ação** para abrir a janela propriedades do computador do cliente.
5. A aba **Aplicativos** na janela propriedades do computador do cliente exibe a lista completa dos aplicativos da Kaspersky Lab instalados no computador do cliente. Selecione **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** na lista de aplicativos.

   Há controles na lista de aplicativos que você pode usar para:

   - exibir a lista de eventos na operação do aplicativo que ocorreram no computador do cliente e foram registrados no Servidor de Administração;
   - exibir as estatísticas atuais em operação de aplicativos;
   - modificar configurações do aplicativo (veja página 119).

INICIAR E INTERROMPER O APLICATIVO

O Kaspersky Anti-Virus 6.0 é instalado e iniciado em computadores de clientes remotos a partir da janela propriedades de aplicativos (consulte a figura abaixo).

No canto superior da janela, você encontrará o nome do aplicativo instalado, informações sobre a versão, data de instalação, o status (se o aplicativo está sendo executado ou foi interrompido no computador local), e informações sobre o status do banco de dados de assinatura de ameaça.
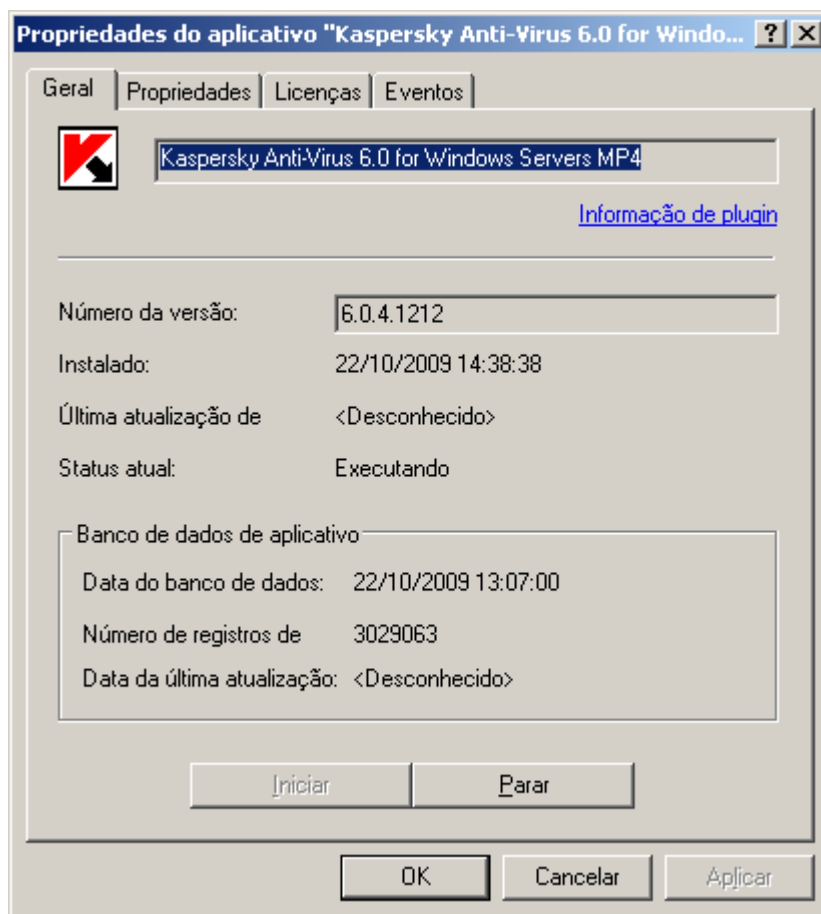
*Figura 13. Janela Propriedades de aplicativos. A aba **Geral***

Para interromper o aplicativo em um computador remoto, faça o seguinte:

1. Abra a janela propriedades do computador de clientes (veja página 116) na aba **Aplicativos**.
2. Selecione **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** na lista de aplicativos e clique no botão **Propriedades**.
3. Na janela propriedades do aplicativo que abrirá, na aba **Geral**, clique no botão **Parar** para interromper o aplicativo e no botão **Iniciar** para iniciá-lo.

CONFIGURAÇÃO DAS CONFIGURAÇÕES DO APLICATIVO

Você pode exibir e editar a janela configurações de aplicativos na aba **Propriedades** de aplicativo (consulte a figura abaixo). As outras abas são padrão para o aplicativo Kaspersky Administration Kit e são contempladas em maiores detalhes no Guia de Referência.
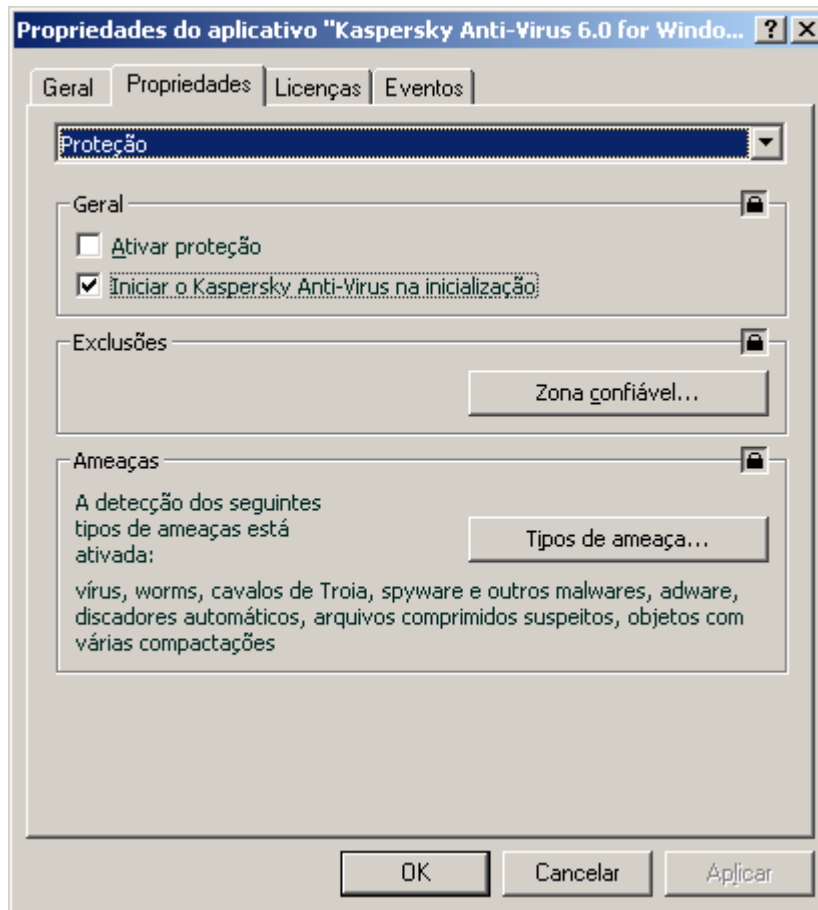
*Figura 14. Janela Propriedades de aplicativos. A aba **Propriedades***

Se uma política tiver sido criada para um aplicativo (veja página 128) que impeça algumas configurações de serem re-modificadas, elas não poderão ser alteradas ao configurar o aplicativo.

Para exibir e editar as configurações aplicativo faça o seguinte:

1. Abra a janela propriedades do computador de clientes (veja página 116) na aba **Aplicativos**.
2. Selecione **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** na lista de aplicativos e clique no botão **Propriedades**.
3. Na janela propriedades do aplicativo que será aberta, na aba **Propriedades** você pode editar os configurações gerais do Antivirus Kaspersky, configurações de armazenamento e relatório, e configurações de rede. Para fazê-lo, selecione o valor desejado do menu suspenso na parte superior da janela, e edite as configurações.

CONSULTE TAMBÉM:

CONFIGURANDO CONFIGURAÇÕES ESPECÍFICAS

Ao administrar o Kaspersky Anti-Virus com o Kaspersky Administration Kit, você poderá ativar/desativar a interatividade, configurar a aparência do aplicativo, e editar informações sobre Suporte Técnico. Essas configurações podem ser editadas na janela propriedades do aplicativo (consulte a figura abaixo).
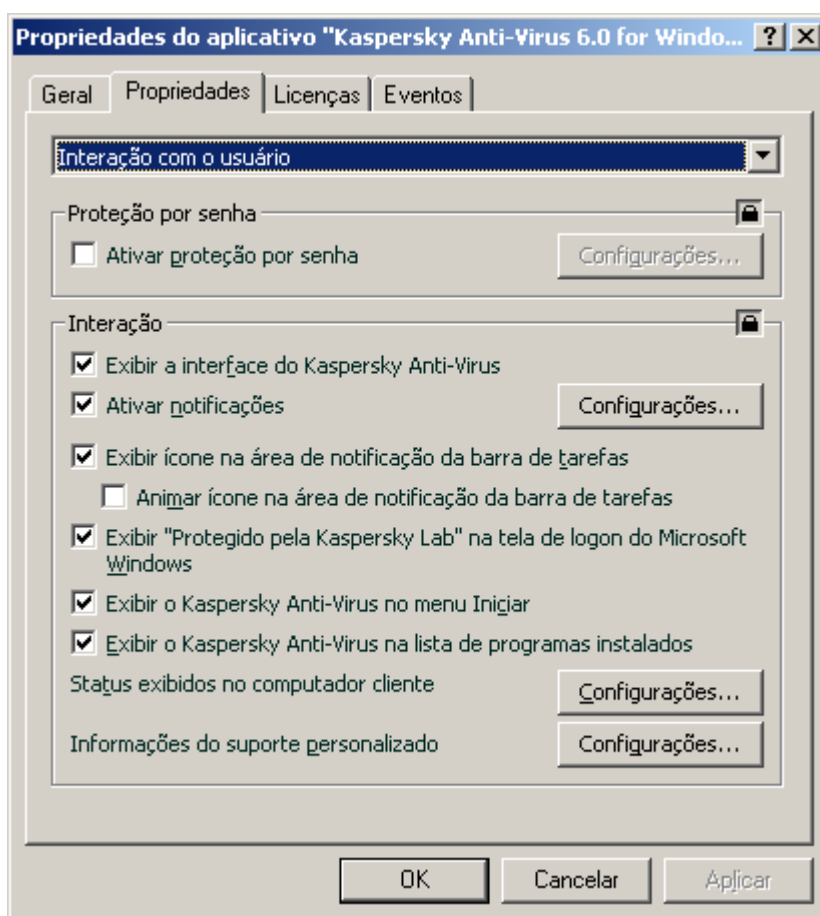
Figura 15. Janela Propriedades de aplicativos. Configurando configurações específicas

Para proteger por senha o Kaspersky Anti-Virus, marque a caixa ☑ **Ativar proteção por senha** na janela que será aberta clicando no botão **Configurações** e insira a senha e a área que será abrangida pela restrição de acesso.

Para configurar a proteção contra a remoção não autorizada de um aplicativo de um computador local, marque a caixa ☑ **Ativar proteção contra desinstalação**. Na janela que será aberta clicando no botão **Configurações**, insira una senha para desinstalar e confirmar.

Para proteger por senha o Kaspersky Anti-Virus, marque a caixa ☑ **Ativar proteção por senha** na janela que será aberta clicando no botão **Configurações** e insira a senha e a área que será abrangida pela restrição de acesso.

Para configurar a proteção contra a remoção não autorizada de um aplicativo de um computador local, marque a caixa ☑ **Ativar proteção contra desinstalação**. Na janela que será aberta clicando no botão **Configurações**, insira una senha para desinstalar e confirmar.

Na seção **Interação**, você pode especificar as configurações de interação do usuário com a interface do Kaspersky Anti-Virus:

- Se a caixa ☐ **Desativar interação** não estiver marcada, um usuário em um computador remoto verá o ícone e mensagens de pop-up Kaspersky Anti-Virus, e terá a possibilidade de tomar decisões sobre ações futuras na janela notificações informando sobre o evento. Para desativar o modo interativo da operação do aplicativo, marque a caixa. Se há necessidade de ocultar a presença do aplicativo ao usuário, marque também a caixa ☑ Ocultar o aplicativo instalado.

- Na janela **Exibir** que será aberta clicando no botão **Configurações**, você pode editar a informação sobre suporte técnico de usuários que é exibida na janela **Suporte** do Kaspersky Anti-Virus.

  Para alterar as informações no campo superior, insira o texto atual sobre o suporte fornecido. No campo abaixo, você pode editar os hiperlinks exibidos na seção **Links úteis** da janela **Suporte** que será aberta ao clicar no link **Suporte** da janela principal do Kaspersky Anti-Virus.

  Edite a lista usando os botões **Adicionar**, **Editar** e **Excluir**. O Kaspersky Anti-Virus adicionará um novo link à parte superior da lista. Para alterar a ordem dos links na lista, use os botões **Mover para cima** e **Mover para baixo**.

  Se a janela não contiver nenhum dado, as informações padrão sobre suporte técnico não estarão sujeitas à edição.

Na seção **Status do aplicativo**, você pode especificar os status do aplicativo que serão exibidos na janela principal do Kaspersky Anti-Virus. Para isso, clique no botão **Configurações** e marque as caixas ☑ para os status requeridos na janela que será aberta. Na mesma janela, você pode especificar os períodos de monitoramento dos bancos de dados do aplicativo.

Na seção **Exibir** você pode editar as configurações para o modo de operação interativa do Kaspersky Anti-Virus em um computador remoto: exibir um ícone sobre a janela de login do Microsoft Windows, o ícone animado do Kaspersky Anti-Virus na bandeja do sistema, emissão de notificações sobre eventos que ocorrem no aplicativo (por exemplo, detecção de um objeto perigoso).

Se uma política tiver sido criada para um aplicativo (veja página 128) que impeça algumas configurações de serem re-modificadas, elas não poderão ser alteradas ao configurar o aplicativo.

➡ *Para exibir e editar as configurações avançadas do aplicativo:*

1. Abra a janela Propriedades do computador de clientes (veja página 116) na aba **Aplicativos**.
2. Selecione **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** na lista de aplicativos e clique no botão **Propriedades**.
3. Na janela propriedades do aplicativo que abrirá, na aba **Propriedades**, selecione o item de **Interação com o usuário** na lista suspensa, e edite as configurações.

GERENCIANDO TAREFAS

Esta seção inclui informações sobre gerenciar tarefas para o Kaspersky Anti-Virus. Para maiores detalhes sobre gerenciar tarefas via Kaspersky Administration Kit, consulte o Guia do Administrador para o produto.

Uma lista de tarefas de sistema é criada para cada computador em rede quando o aplicativo está sendo instalado. Esta lista inclui tarefas de proteção (Antivírus de arquivos), tarefas de verificação de vírus (Verificação completa, Verificação rápida) y tarefas de atualização (atualizações e módulos dos bancos de dados do aplicativo, atualização de reversões).

Você também pode gerenciar a programação para tarefas de sistema e editar as respectivas configurações. Essas tarefas não podem ser excluídas.

Você também pode criar suas próprias tarefas (veja página 123), tal como tarefas de verificação, atualizações de aplicativo e atualizar reversões, e as tarefas de instalação do arquivo de chave.
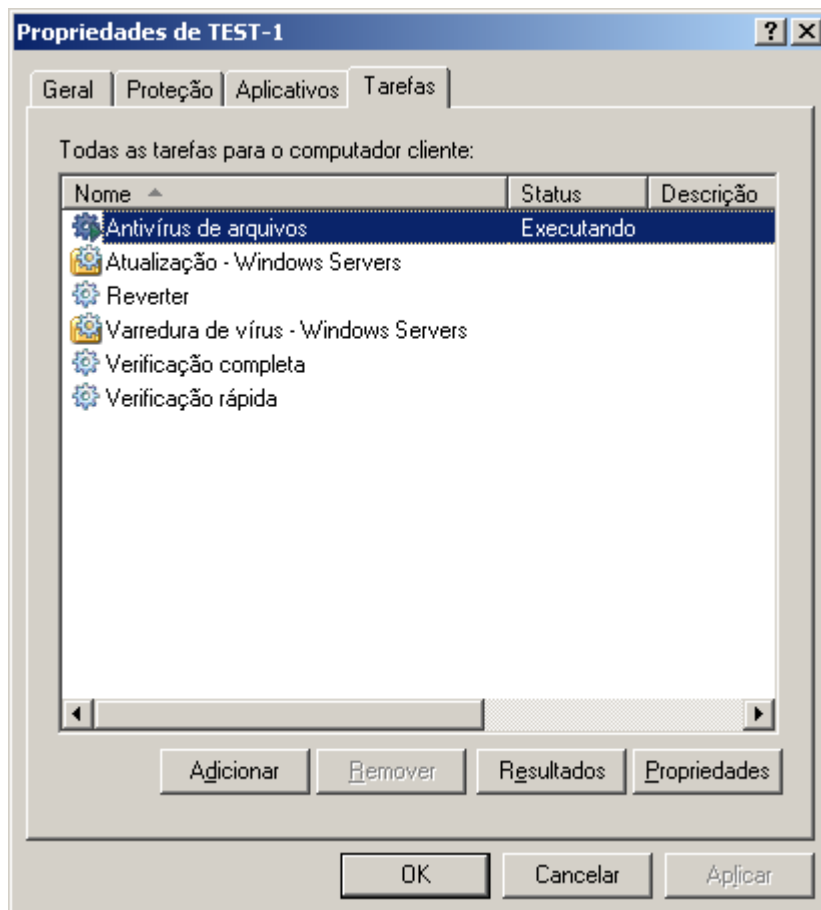
Figura 16. Janela de propriedades do computador do cliente. A aba ***Tarefas***

Para abrir a lista de tarefas criada para o computador de um cliente:

1. Abra o Kaspersky Administration Kit.
2. Selecionar a pasta **Computadores gerenciados** com o nome do grupo que inclui o computador do cliente.
3. No grupo selecionado, abrir a pasta **computadores do Cliente** e selecionar o computador no qual você precisa modificar as configurações do aplicativo.
4. Selecionar o comando **Propriedades** do menu contexto ou o item correspondente do menu **Ação** para abrir a janela propriedades do computador do cliente.
5. Na janela propriedades de computador do cliente que abrirá, selecione a aba **Tarefas**. Aqui, você encontrará a lista completa das tarefas criadas para o computador do cliente.

INICIAR E INTERROMPER TAREFAS

As Tarefas são iniciadas no computador do cliente apenas se o aplicativo correspondente estiver sendo executado (veja página 117). Se o aplicativo for interrompido, todas as tarefas sendo executadas serão encerrados.

As tarefas são iniciadas e interrompidas automaticamente, de acordo com a programação, ou manualmente usando os comandos do meu contexto e da janela Exibir Configurações de Tarefas. Você também pode pausar e reiniciar as mesmas.

Para iniciar/interromper/pausar/reiniciar uma tarefa manualmente:

1. Abra a janela de propriedades do computadordo cliente na aba **Tarefas**.
2. Selecione a tarefa desejada e abra o menu contexto para ela. Selecione o item **Iniciar** e inicie a tarefa ou o item **Interromper** para interrompê-la. Você também pode usar os itens correspondentes no menu **Ação**.

   Você não pode pausar nem reiniciar uma tarefa do menu contexto.Exibindo o aplicativo no Menu Iniciar.

   ou

   Selecione a tarefa desejada na lista e clique no botão **Propriedades**. Você pode usar os botões na aba **Geral** na janela propriedades de tarefas que abrirá para iniciar, interromper, pausar ou reiniciar uma tarefa.

CRIAR TAREFAS

Ao trabalhar com o aplicativo via Kaspersky Administration Kit, você poderá criar os seguintes tipos de tarefas:

- tarefas locais definidas de computadores de clientes individuais;
- tarefas de grupo para computadores de clientes que pertencem aos grupos de administração;
- tarefas para conjuntos de computadores definidos para computadores fora dos grupos de administração;
- As tarefas do Kaspersky Administration são tarefas específicas para o Servidor de Atualização: atualizar baixar tarefas, tarefas de backup, e reportar o envio de tarefas.

  Grupos de computador apenas só são executados no conjunto selecionado de computadores. Se novos computadores de clientes forem adicionados a um grupo com computadores para os quais uma tarefa de instalação remota foi criada, essa tarefa não será executada para eles. Você deve criar uma nova tarefa ou efetuar as alterações apropriadas às configurações da tarefa atual.

Você pode executar as seguintes ações em tarefas:

- especificar ajustes de tarefas;
- monitorar a execução de tarefas;
- copiar e mover tarefas de um grupo para outro, e também excluí-las usando os comandos padrão **Copiar/Colar, Recortar/Colar, Excluir** do menu contexto, ou os mesmos comandos do menu **Ação**;
- importar e exportar tarefas.

Consultar o Guia de Referência do Kaspersky Administration Kit para maiores informações sobre trabalhar com tarefas.

Para criar uma tarefa local:

1. Abrir a janelade propriedades do computador do cliente requerido, na aba **Tarefas**.

2. Clique no botão **Adicionar**.

3. O Assistente de Nova Tarefa iniciará (veja página 124). Siga suas instruções.

Para criar uma tarefa de grupo:

1. Abra o Console de Administração do Kaspersky Administration Kit.

2. Na pasta **Computadores gerenciados**, abra a pasta com nome do grupo desejado.

3. No grupo que você selecionou, abra a pasta **Tarefas do grupo**, onde você encontrará todas as tarefas criadas para o grupo.

4. Abrir o Assistente de Nova Tarefa clicando em **Criar um link de nova tarefa** na barra de tarefas. Os detalhes para criar tarefas de grupo são contemplados no Guia de Referência do Kaspersky Administration Kit.

Para criar uma tarefa para um grupo de computadores (uma tarefa do Kaspersky Administration Kit):

1. Abra o Kaspersky Administration Kit.

2. Selecione as **Tarefas para a pasta computadores específicos** (t**arefas do Kaspersky Administration Kit**).

3. Abrir o Assistente de Nova Tarefa clicando em **Criar um link de nova tarefa** na barra de tarefas. Os detalhes para criar tarefas do Kaspersky Administration Kit e tarefas para grupos de computadores são contemplados no Guia de Referência do Kaspersky Administration Kit.

ASSISTENTE DE TAREFA LOCAL

O Assistente de Tarefa Local inicia quando você seleciona os comandos correspondentes do menu contexto para o computador do cliente ou da janela propriedades para aquele computador.

Esse assistente consiste de uma série de caixas (passos) navegados com o uso dos botões **Avançar** e **Voltar**. Para fechar o assistente quando ele completar o trabalho, use o botão **Concluir**. Para cancelar o assistente a qualquer momento, use o botão **Cancelar**.

ETAPA 1. INSERIR DADOS GERAIS NA TAREFA

A primeira janela do assistente é introdutória: tudo o que você insere aqui é o nome da tarefa (o campo **Nome**).

ETAPA 2. SELECIONANDO UM APLICATIVO E TIPO DE TAREFA

Nessa etapa, você deve especificar o aplicativo para o qual a tarefa está sendo criada (Kaspersky Anti-Virus 6.0 para Windows Servers MP4, ou Agente de Administração). Você também deve selecionar o tipo de tarefa. As possíveis tarefas do Kaspersky Anti-Virus 6.0 são:

- *Verificar vírus* – tarefa de verificação de vírus das áreas especificadas pelo usuário.
- *Atualizar* – recupera e aplica os pacotes de atualização para o aplicativo.
- *Atualizar Reversão* – reverte a última atualização do aplicativo.
- *Instalação do arquivo de chave* – instalação de um arquivo de chave para uma nova licença conforme necessário para operar esse aplicativo.

ETAPA 3. CONFIGURANDO O TIPO DE TAREFA SELECIONADA

Dependendo do tipo da tarefa na etapa anterior, o conteúdo da janela configurações poder variar.

As tarefas de verificação de vírus requerem que você especifique a ação que o Kaspersky Anti-Virus executará se detectar um objeto malicioso (veja página 50) e requer que você crie uma lista de objetos a serem verificados (veja página 49).

Para as tarefas de atualização do bancos de dados e módulo de aplicativo, você deverá especificar a fonte que usará para baixar as atualizações (veja página 61). A fonte de atualização padrão é o servidor de atualização do Kaspersky Administration Kit.

Atualizar tarefas de reversão que não tenham configurações específicas.

Para tarefas de instalação de chave, especificar o caminho para o arquivo de chave com o botão **Procurar**. Para adicionar um arquivo como chave de licença para uma licença adicional, marque a ☑ caixa correspondente. A chave de licença adicional entrará em vigor quando a chave de licença ativa expirar.

Informações sobre a licença especificadas (número de licença, tipo e data de expiração) são exibidas no campo abaixo.

ETAPA 4. CONFIGURANDO UMA PROGRAMAÇÃO

Depois de configurar as tarefas, lhe será oferecido configurar a programação execução de tarefa automática.

Para fazê-lo, selecione a freqüência para executar a tarefa no menu suspenso nas configurações de programação na parte inferior da janela.

ETAPA 5. CONCLUINDO A CRIAÇÃO DE TAREFAS

A última janela do assistente informará a você se criou a tarefa com êxito.

CONFIGURANDO TAREFAS

A configuração de tarefas do aplicativo através da interface do Kit de Administração Kaspersky é semelhante à configuração através da interface do Antivirus Kaspersky, exceto pelos ajustes que são editados individualmente para cada usuário, como esquemas de execução de tarefas de verificação, ou configurações específicas do Kit de Administração Kaspersky, como configurações que permitem/bloqueiam o gerenciamento de tarefas de verificação local pelo usuário.

Se uma política tiver sido criada para um aplicativo (veja página 128) que impeça algumas configurações de serem re-modificadas, elas não poderão ser alteradas ao configurar o aplicativo.

Todas as abas da janela propriedades além da aba **Propriedades** (consulte a figura abaixo) são padrão para o Kaspersky Administration Kit e são contempladas em maiores detalhes no Guia de Referência. A aba **Propriedades** contém configurações específicas para o Kaspersky Anti-Virus. O conteúdo dessa aba variar dependendo do tipo de tarefa selecionada.
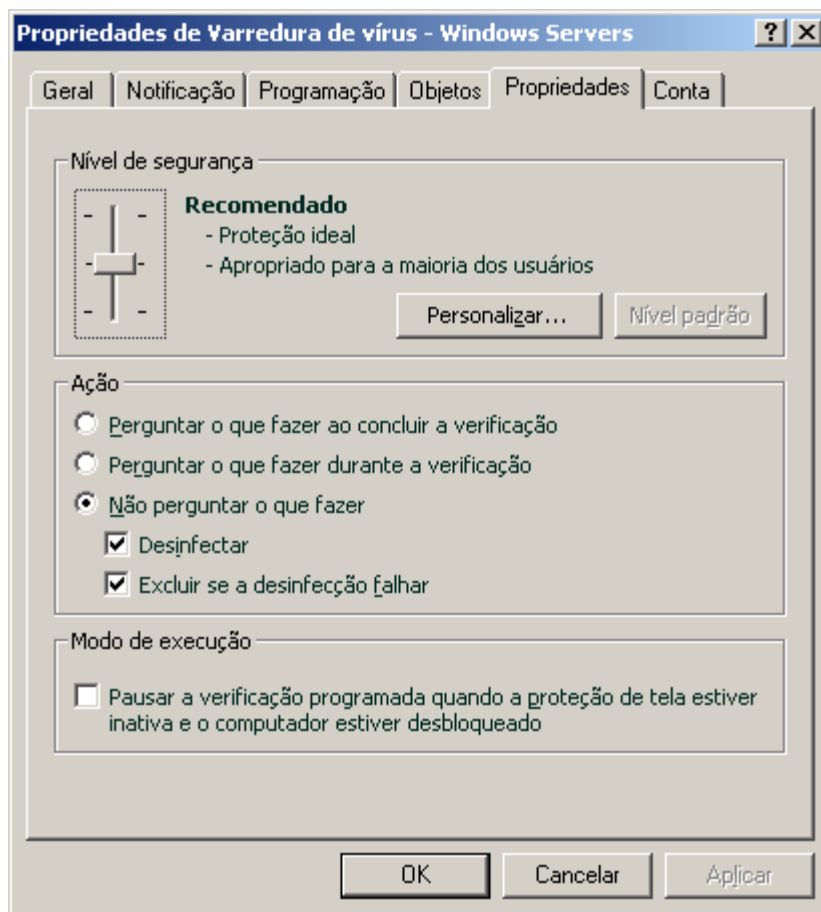
*Figura 17. Janela Propriedades de tarefas. A aba **Propriedades***

➧ *Para exibir e editar tarefas locais, faça o seguinte:*

1. Abra a janela Propriedades do computador de clientes na aba **Tarefas**.
2. Selecione a tarefa na lista e clique no botão **Propriedades**. Como resultado, a janela configurações de tarefas abrirá.

➧ *Para exibir tarefas de grupo:*

1. Abra o Kaspersky Administration Kit.
2. Na pasta **Computadores gerenciados**, abra a pasta com nome do grupo desejado.
3. No grupo que você selecionou, abra a pasta **Tarefas do grupo**, onde você encontrará todas as tarefas criadas para o grupo.
4. Selecione a tarefa desejada da árvore do console para exibir e editar as propriedades.

   A barra de tarefas exibirá informações abrangentes sobre a tarefa e os links para gerenciar a execução e edição de tarefas e editar as suas configurações. Os detalhes para criar tarefas de grupo são descritas no Guia de Referência do Kaspersky Administration Kit.

➡ *Para exibir tarefas para um grupo de computadores (uma tarefa do Kaspersky Administration Kit):*

1. Abra o Kaspersky Administration Kit.
2. Selecione as **Tarefas para a pasta computadores específicos** (t**arefas do Kaspersky Administration Kit**).
3. Selecione a tarefa desejada da árvore do console para exibir e editar as propriedades.

   A barra de tarefas exibirá informações abrangentes sobre a tarefa e os links para gerenciar a execução e edição de tarefas e editar as suas configurações. Os detalhes das tarefas do Kaspersky Administration Kit e tarefas para grupos de computadores podem ser encontrados Guia de Referência do Kaspersky Administration Kit.

GERENCIAMENTO DE POLÍTICAS

Estabelecer políticas permite que você aplique configurações de aplicativo e tarefas universais para clientes de computadores que pertençam a um único grupo de administração.

Esta seção inclui informações sobre criar e configurar políticas para o Kaspersky Anti-Virus 6.0 para Windows Servers MP4. Para maiores detalhes sobre o conceito de políticas de administração através do Kaspersky Administration Kit, consulte o Guia do Administrador para o aplicativo.

Ao criar e configurar uma política, você pode bloquear total ou parcialmente configurações de serem editadas para grupos aninhados, configurações de tarefas, e configurações de aplicativos. Para fazê-lo, clique no botão . Ele deve alternar para configurações travadas.

➡ *Para abrir a lista de políticas para o Kaspersky Anti-Virus, faça o seguinte:*

1. Abra o Kaspersky Administration Kit.
2. Selecionar a pasta **Computadores gerenciados** com o nome do grupo que inclui o computador do cliente.
3. No grupo que você selecionou, abra a pasta **Políticas**, onde você encontrará todas as políticas criadas para o grupo.

CRIANDO POLÍTICAS

Ao trabalhar com o Kaspersky Anti-Virus via Kaspersky Administration Kit, você pode criar os seguintes tipos de políticas:

Você pode executar as seguintes ações em políticas:

- configurando políticas;
- copiar e mover políticas de um grupo para outro, e também excluí-las usando os comandos padrão **Copiar/Colar, Recortar/Colar, Excluir** do menu contexto, ou os mesmos comandos do menu **Ação**;
- importando e exportando configurações de políticas.

Trabalhando com políticas contempladas em maiores detalhes no Guia de Referência do Kaspersky Administration Kit.

➡ *Para criar uma política, faça o seguinte:*

1. Abra oConsole de Administração do Kaspersky Administration Kit.
2. Na pasta **Computadores gerenciados**, abra a pasta com nome do grupo desejado.

3. No grupo que você selecionou, abra a pasta **Políticas**, onde você encontrará todas as políticas criadas para o grupo.

4. Abra o Assistente de Nova Tarefa clicando em **Criar um link de nova política** na barra de tarefas.

5. O Novo Auxiliar de Tarefas iniciará na janela que se abre (veja página 128) e siga as instruções.

ASSISTENTE DE CRIAÇÃO DE POLÍTICA

O Assistente de Política pode ser iniciado selecionando a ação correspondente do menu contexto da pasta **Políticas** do grupo de administração desejado, ou clicando no link no painel de resultados (para as pastas **Políticas**).

Esse assistente consiste de uma série de caixas (passos) navegados com o uso dos botões **Avançar** e **Voltar**. Para fechar o assistente quando ele completar o trabalho, use o botão **Concluir**. Para cancelar o assistente a qualquer momento, use o botão **Cancelar**.

ETAPA 1. INSERIR DADOS GERAIS NA POLÍTICA

As janelas do primeiro assistente são janelas de boas vindas. Aqui, você deve especificar o nome da política (o campo **Nome**) e selecionar **Kaspersky Anti-Virus 6.0 para Windows Servers MP4** do menu suspenso do **nome do Aplicativo**.

Se você executar o Assistente de Criação de **Política** do nódulo da barra de tarefas (usando **Criar uma nova política Kaspersky Anti-Virus para Windows Servers MP4**), você não poderá selecionar um aplicativo.

Se você quiser criar uma política baseada nas definições da política atual para a versão anterior do aplicativo, marque a caixa ☑ **Tomar as configurações da de política atual** e selecione a política cujas configurações devem ser usadas na nova política. Para selecionar uma política, clique no botão **Selecionar**, que abrirá a lista de políticas atuais que você poderá usar ao criar uma nova política.

ETAPA 2. SELECIONANDO O STATUS DA POLÍTICA

Nesta janela, você poderá especificar o status da política após ela ser criada, selecionando uma das seguintes opções: política ativa ou política inativa. Consultar o Guia de Referência do Kaspersky Administration Kit para maiores detalhes sobre status de política.

Várias políticas podem ser criadas para um único aplicativo em um grupo, mas apenas uma delas pode ser a política atual (ativa).

ETAPA 3. IMPORTANDO AS CONFIGURAÇÕES DE APLICATIVOS

Se você tiver um arquivo com os ajustes de aplicativo salvos anteriormente, poderá especificar o caminho utilizando o botão **Carregar**; as janelas do auxiliar exibidas mostrarão os ajustes importados.

ETAPA 4. CONFIGURANDO A PROTEÇÃO

Nesta etapa, você poder ativar/desativar ou configurar componentes de proteção que serão usados na política.

Todos os componentes de proteção são ativados por padrão. Para desativar os componentes, desmarque as caixas ao lado. Para sintonizar o componente de proteção, selecione-o da lista e clique no botão **Configurar**.

ETAPA 5. CONFIGURANDO PROTEÇÃO DE SENHA

Nesta janela do assistente, você poderá configurar a proteção por senha aplicada a operações com o aplicativo e a desinstalação.

ETAPA 6. CONFIGURANDO A ZONA CONFIÁVEL

Nesta janela do assistente, você poderá configurar a zona confiável: adicione o software usado para administração de rede à lista de aplicativos confiáveis, e exclua vários tipos de arquivo da verificação.

ETAPA 7. CONFIGURANDO INTERAÇÃO COM O USUÁRIO

Nesta etapa, você poderá especificar as configurações para interação entre o usuário e o Kaspersky Anti-Virus:

- exibindo a interface do aplicativo em um computador remoto;
- notificando o usuário sobre eventos;
- exibindo o ícone do aplicativo na área de notificação da barra de tarefas e animando-o;
- exibindo "Protegido pela Kaspersky Lab" na tela de logon do Microsoft Windows;
- exibindo o aplicativo no Menu Iniciar;
- exibindo o aplicativo na lista de aplicativos instalados.

ETAPA 8. CONCLUINDO A CRIAÇÃO DE POLÍTICAS

A última janela do assistente informará a você se criou a política com êxito.

Quando o assistente estiver fechado, a política do aplicativo será adicionada à pasta **Políticas** do grupo correspondente, ficando visível na árvore do console.

Você poderá editar as configurações de políticas criadas e definir restrições ao modificar suas configurações usando o e botões para cada grupo de configurações. Se o ícone for exibido, o computador do cliente não será capaz de editar as configurações. Se o ícone for exibido, o usuário será capaz de editar as configurações. A política será aplicada aos computadores do cliente na primeira vez que os clientes se sincronizarem ao servidor.

CONFIGURANDO A POLÍTICA

Na etapa de edição, você poderá modificar a política e bloquear a modificação das configurações em políticas aninhadas de grupo, e nas configurações de aplicativos e tarefas. As configurações de políticas podem ser editadas na janela propriedades de políticas (consulte a figura abaixo).
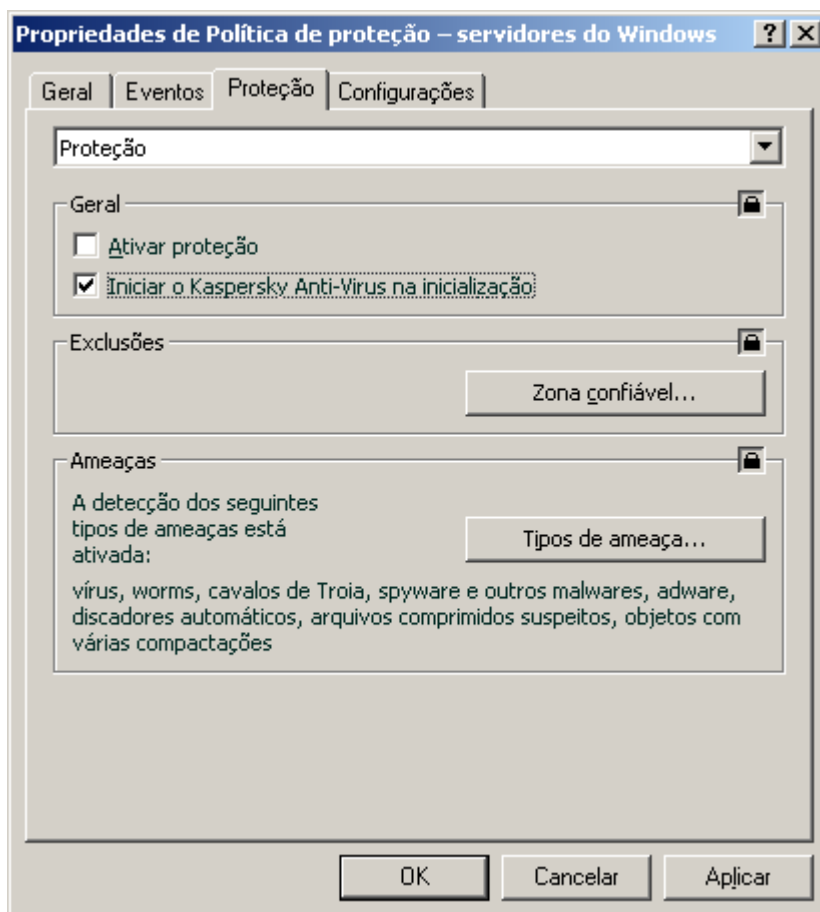
*Figura 18. Janela Propriedades de políticas. A aba **Proteção***

Todas as abas, exceto as abas **Proteção** e **Configurações**, são padrão para o Kaspersky Administration Kit. Elas são cobertas em maiores detalhes no Guia do Administrador.

As configurações de política para o Kaspersky Anti-Virus 6.0 incluem configurações de aplicativos (veja página 119) e configurações de tarefas. A aba **Configurações** exibe as configurações de aplicativos e a aba **Proteção** exibe as configurações de tarefas.

Para editar as configurações, selecione o valor desejado do menu suspenso na parte superior da janela, e configure-o.

➧ *Para exibir e editar políticas locais, faça o seguinte:*

1. Abra o Kaspersky Administration Kit.
2. Na pasta **Computadores gerenciados**, abra a pasta com nome do grupo desejado.
3. No grupo que você selecionou, abra a pasta **Políticas**, onde você encontrará todas as políticas criadas para o grupo.
4. Selecionar a política desejada da árvore do console para exibir e editar as propriedades.
5. A barra de tarefas exibirá informações abrangentes sobre a política e os links para gerenciar o status da política e editar as suas configurações.

ou

Abrir o menu contexto da política selecionada e usar o item **Propriedades** para abrir a janela Configurações de políticas do Kaspersky Anti-Virus.

Os detalhes para trabalhar com políticas podem ser encontrados no Guia de Referência do Kaspersky Administration Kit.

USANDO CÓDIGO DE TERCEIROS

Foi utilizado código de terceiros no desenvolvimento do Kaspersky Internet Security.

NESTA SEÇÃO

BIBLIOTECA BOOST 1.30

Ao criar o aplicativo, a biblioteca Boost 1.30 foi utilizada. Copyright (C) 2003, Christof Meerwald.

BIBLIOTECA LZMA SDK 4.40, 4.43

Ao criar o aplicativo, a biblioteca LZMA SDK 4,40, 4,43 foi utilizada. Copyright (C) 1999-2006, Igor Pavlov.

BIBLIOTECA OPENSSL-0.9.8D

A biblioteca OPENSSL-0.9.8D foi usada no desenvolvimento do aplicativo. Copyright (C) 1998-2007 The OpenSSL Project.

LICENSE

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org).

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

BIBLIOTECA WINDOWS TEMPLATE LIBRARY (WTL 7.5)

Ao criar o aplicativo, a biblioteca Windows Template Library 7.5 foi utilizada. Copyright (C) 2006, Microsoft Corporation.

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. **Definições**

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. **Grant of Rights**

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. **Conditions and Limitations**

   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   (E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

BIBLIOTECA WINDOWS INSTALLER XML (WIX-2.0)

Ao criar o aplicativo, a biblioteca de ferramentas do Windows Installer XML (WiX) foi utilizada. Copyright (C) 2009, Microsoft Corporation.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

a. in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b. in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

   If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

   If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

   All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

   Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

   This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTECA ZIP-2.31

Ao criar o aplicativo, a biblioteca ZIP-2.31 foi utilizada. Copyright (C) 1990-2005, Info-ZIP.

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTECA ZLIB-1.0,4, ZLIB-1.1,3, ZLIB-1.2.3

Ao criar o aplicativo, a biblioteca ZLIB-1.0,4, ZLIB-1.1,3, ZLIB-1.2,3 foi utilizada. Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

BIBLIOTECA UNZIP-5.51

Ao criar o aplicativo, a biblioteca UNZIP-5.51 foi utilizada. Copyright (c) 1990-2004 Info-ZIP.

This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg

Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTECA LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12

Ao criar o aplicativo, a biblioteca LIBPNG-1.0,1, LIBPNG-1.2,8, LIBPNG-1.2,12 foi utilizada.

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, August 15, 2004, through 1.2.39, August 13, 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

BIBLIOTECA LIBJPEG-6B

Ao criar o aplicativo, a biblioteca LIBJPEG-6B foi utilizada. Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

LEGAL ISSUES

============

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch,

sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead

by the usual distribution terms of the Free Software Foundation; principally,

that you must include source code if you redistribute it. (See the file

ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part

of any program generated from the IJG code, this does not limit you more than

the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

> "The Graphics Interchange Format(c) is the Copyright property of
>
> CompuServe Incorporated. GIF(sm) is a Service Mark property of
>
> CompuServe Incorporated."

BIBLIOTECA LIBUNGIF-4.1.4

Ao criar o aplicativo, a biblioteca LIBUNGIF-4.1.4 foi utilizada. Copyright (C) 1997 Eric S. Raymond.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

BIBLIOTECA PCRE 3.0

A biblioteca PCRE 3.0 foi usada no desenvolvimento do aplicativo. Copyright (C) 1997-1999, University of Cambridge.

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2000 University of Cambridge

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. If PCRE is embedded in any software that is released under the GNU General Purpose Licence (GPL), then the terms of that licence shall supersede any condition above with which it is incompatible.

End

BIBLIOTECA REGEX-3.4A

A biblioteca REGEX-3.4A foi usada no desenvolvimento do aplicativo. Copyright (C) 1992, 1993, 1994, 1997, Henry Spencer.

This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.

4. This notice may not be removed or altered.

BIBLIOTECA MD5 MESSAGE-DIGEST ALGORITHM-REV. 2

Ao criar o aplicativo, a biblioteca MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 foi utilizada.

BIBLIOTECA MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004

Ao criar o aplicativo, a biblioteca MD5 MESSAGE-DIGEST ALGORITHM-V. 18,11.2004 foi utilizada.

BIBLIOTECA INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999

Ao criar o aplicativo, a biblioteca INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04,11.1999 foi utilizada.

RSA's MD5 disclaimer

BIBLIOTECA CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004

A biblioteca CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 foi usada no desenvolvimento do aplicativo.

Disclaimer

Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

BIBLIOTECA COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM

Ao criar o aplicativo, a biblioteca COOL OWNER DRAWN MENUS-V. 2,4, 2,63 By Brent Corkum foi utilizada.

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware,Shareware,Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

BIBLIOTECA LIBJPEG FMT-2002

A biblioteca FMT-2002 foi usada no desenvolvimento do aplicativo. Copyright (C) 2002, Lucent Technologies.

The authors of this software are Rob Pike and Ken Thompson.Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

BIBLIOTECA EXPAT-1.95.2

A biblioteca EXPAT-1.95.2 foi usada no desenvolvimento do aplicativo. Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTECA LIBJPEG LIBNKFM-0.1

A biblioteca LIBNKFM-0.1 foi usada no desenvolvimento do aplicativo. Copyright (C) 1987, Fujitsu LTD (Itaru ICHIKAWA).

Everyone is permitted to do anything on this program including copying, modifying, improving, as long as you don't try to pretend that you wrote it. i.e., the above copyright notice has to appear in all copies. Binary distribution requires original version messages. You don't have to ask before copying, redistribution or publishing.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE.

BIBLIOTECA PLATFORM INDEPENDENT IMAGE CLASS

Ao criar o aplicativo, a biblioteca PLATFORM INDEPENDENT IMAGE CLASS foi utilizada. Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx).

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BIBLIOTECA NETWORK KANJI FILTER (PDS VERSION)-2.0.5

A biblioteca NETWORK KANJI FILTER (PDS VERSION)-2.0.5 foi usada no desenvolvimento do aplicativo. Copyright (C) 1987, Fujitsu LTD. (Itaru ICHIKAWA).

Everyone is permitted to do anything on this program including copying, modifying, improving, as long as you don't try to pretend that you wrote it. i.e., the above copyright notice has to appear in all copies. Binary distribution requires original version messages. You don't have to ask before copying, redistribution or publishing.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE.

BIBLIOTECA DB-1.85

A biblioteca DB-1.85 foi usada no desenvolvimento do aplicativo. Copyright (C) 1990, 1993, 1994, The Regents of the University of California.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTECA LIBNET-1991, 1993

A biblioteca LIBNET-1991,1993 foi usada no desenvolvimento do aplicativo. Copyright (C) 1991, 1993, The Regents of the University of California.

This code is derived from software contributed to Berkeley by Berkeley Software Design, Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTECA GETOPT-1987, 1993, 1994

A biblioteca GETOPT-1987, 1993, 1994 foi usada no desenvolvimento do aplicativo. Copyright (C) 1987, 1993, 1994, The Regents of the University of California.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTECA MERGE-1992, 1993

A biblioteca MERGE-1992, 1993 foi usada no desenvolvimento do aplicativo. Copyright (C) 1992, 1993, The Regents of the University of California.

This code is derived from software contributed to Berkeley by Peter McIlroy.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTECA FLEX PARSER (FLEXLEXER)-V. 1993

Ao criar o aplicativo, a biblioteca FLEX PARSER (FLEXLEXER)-V. 1993 foi utilizada. Copyright (c) 1993 The Regents of the University of California.

This code is derived from software contributed to Berkeley by Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

BIBLIOTECA STRPTIME-1.0

A biblioteca STRPTIME-1.0 foi usada no desenvolvimento do aplicativo. Copyright (C) 1994, Powerdog Industries.

Redistribution and use in source and binary forms, without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by Powerdog Industries.

4. The name of Powerdog Industries may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY POWERDOG INDUSTRIES ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE POWERDOG INDUSTRIES BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE

BIBLIOTECA ENSURECLEANUP, SWMRG, LAYOUT-V. 2000

Ao criar o aplicativo, a biblioteca ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 foi utilizada. Copyright (C) 2009, Microsoft Corporation.

NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software ("License Agreement").

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as "sample" available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252,227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52,227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

BIBLIOTECA OUTLOOK2K ADDIN-2002

A biblioteca OUTLOOK2K ADDIN-2002 foi usada no desenvolvimento do aplicativo. Copyright (C) 2002, Amit Dey email: amitdey@joymail.com.

This code may be used in compiled form in any way you desire. This file may be redistributed unmodified by any means PROVIDING it is not sold for profit without the authors written consent, and providing that this notice and the authors name is included.

This file is provided 'as is' with no expressed or implied warranty. The author accepts no liability if it causes any damage to your computer.

Do expect bugs.

Please let me know of any bugs/mods/improvements.

and I will try to fix/incorporate them into this file.

Enjoy!

BIBLIOTECA STDSTRING- V. 1999

Ao criar o aplicativo, a biblioteca STDSTRING-V. 1999 foi utilizada. Copyright (C) 1999, Joseph M. O'Leary.

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes your $30 billion dollar satellite explode in orbit. If you redistribute it in any form, I'd appreciate it if you would leave this notice here.

T-REX (TINY REGULAR EXPRESSION LIBRARY)-V. 2003-2006

Ao criar o aplicativo, a biblioteca T-REX (TINY REGULAR EXPRESSION LIBRARY)-V foi utilizada. Copyright (C) 2003-2006, Alberto Demichelis.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BIBLIOTECA NTSERVICE- V. 1997

Ao criar o aplicativo, a biblioteca NTSERVICE-V. 1997 foi utilizada. Copyright (C) 1997 by Joerg Koenig and the ADG mbH, Mannheim, Germany.

Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY "//!! TCW MOD"

BIBLIOTECA SHA-1-1.2

Ao criar o aplicativo, a biblioteca SHA-1-1.2 foi utilizada. Copyright (C) 2001, The Internet Society.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

BIBLIOTECA COCOA SAMPLE CODE- V. 18.07.2007

Ao criar o aplicativo, a biblioteca Cocoa sample code- v. 18.07.2007 foi utilizada. Copyright (C) 2007, Apple Inc.

BIBLIOTECA PUTTY SOURCES-25.09.2008

Ao criar o aplicativo, a biblioteca PUTTY SOURCES-25.09.2008 foi utilizada. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified http://www.opensource.org/licenses/ and complies with the Debian Free Software Guidelines http://www.debian.org/social_contract)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

OUTRAS INFORMAÇÕES

O Aplicativo pode incluir alguns programas de aplicativo que são licenciados (ou sublicenciados) para o usuário sob Licença Pública Geral GNU (GNU General Public License, GPL) ou outras licenças similares de aplicativo livre, que, entre outros direitos, permitem ao usuário copiar, modificar e redistribuir determinados programas, ou partes dos mesmos, bem como ter acesso ao código-fonte (Aplicativo com Código Aberto). Caso essas licenças exijam que, para qualquer aplicativo que é distribuído a alguém em formato binário executável, o código-fonte também seja disponibilizado a esses usuários, então ele deve ser disponibilizado por meio do envio de uma solicitação para source@kaspersky.com.

GLOSSÁRIO

A

ALARME FALSO

Situação em que o aplicativo da Kaspersky Lab considera um objeto não infectado como infectado devido ao seu código similar ao de um vírus.

ANALISADOR HEURÍSTICO

Tecnologia de detecção de ameaças que não podem ser detectadas usando os bancos de dados de antivírus. Permite a detecção de objetos suspeitos de infecção por um vírus desconhecido ou por uma nova modificação dos vírus conhecidos.

Com o analisador heurístico, até 92% das ameaças são detectadas. Esse mecanismo é bastante eficiente e raramente produz falsos positivos.

Os arquivos detectados pelo analisador heurístico são considerados suspeitos.

APLICATIVO INCOMPATÍVEL

Um aplicativo de antivírus de um terceiro desenvolvedor ou um aplicativo da Kaspersky Lab que não suporta gerenciamento pelo Kaspersky Administration Kit.

ARMAZENAMENTO DE BACKUP

Uma pasta de armazenamento especial para cópias de dados do Servidor de Administração criadas usando um utilitário de backup.

ARQUIVO

Arquivos que "contêm" um ou vários outros objetos que também podem ser arquivos.

ARQUIVO COMPRIMIDO

Um arquivo que contém um programa de descompressão e instruções para sistema operacional para execução.

ARQUIVO DE CHAVE

Arquivo com a extensão .key, que é sua "chave" pessoal, necessário para trabalhar com o aplicativo da Kaspersky Lab. Um arquivo de chave é incluído com o produto se você o comprou de distribuidores da Kaspersky Lab ou se foi enviado por email a você, caso você tenha comprado o produto na eStore.

ATUALIZAÇÃO

O procedimento de substituição/adicionamento de novos arquivos (bancos de dados ou módulos de aplicativos) recuperados pelos servidores de atualização da Kaspersky Lab.

ATUALIZAÇÕES DE BANCOS DE DADOS

Uma das funções executadas pelo aplicativo da Kaspersky Lab que permite à mesma manter a proteção atualizada. Ao fazê-lo, os bancos de dados são baixados dos servidores de atualização da Kaspersky Lab para o computador e automaticamente conectados ao aplicativo.

ATUALIZAÇÕES DISPONÍVEIS

Um conjunto de módulo do aplicativo da Kaspersky Lab que inclui atualizações críticas acumuladas em um período de tempo e alterações à arquitetura do aplicativo.

ATUALIZAÇÕES URGENTES

Atualizações críticas de módulos de aplicativos da Kaspersky Lab.

B

BACKUP

Armazenamento especial para salvar cópias de backup de objetos criados antes da primeira desinfecção ou exclusão.

BANCOS DE DADOS

Bancos de dados criados pelos especialistas da Kaspersky Lab, que contêm descrições detalhadas de todas as ameaças à segurança de computadores existentes atualmente, além dos métodos usados para sua detecção e desinfecção. Esses bancos de dados são atualizados pela Kaspersky Lab constantemente conforme surgem novas ameaças. Para obter uma detecção de ameaças de alta qualidade, é recomendável copiar os bancos de dados dos servidores de atualização da Kaspersky Lab periodicamente.

BLOQUEANDO O OBJETO

Negando acesso a um objeto de aplicativos externos. Um objeto bloqueado não pode ser lido, executado, alterado nem excluído.

C

CABEÇALHO

As informações no início de um arquivo ou mensagem, que compreendem dados de nível baixo status e processamento de um arquivo (ou mensagem). Em particular, o cabeçalho do email contém tais dados como informações sobre o remetente e o destinatário, e a data.

CÓPIA DE BACKUP

Criação de uma cópia de backup de um arquivo antes do processamento e colocação dessa cópia na área de armazenamento de backup, com a possibilidade de restaurar o arquivo posteriormente, por exemplo, para verificá-lo com bancos de dados atualizados.

D

DESINFECÇÃO DE OBJETOS

Método usado para processar objetos infectados que resulta na recuperação completa ou parcial dos dados, ou na decisão de que os objetos não podem ser desinfetados. A desinfecção de objetos é executada usando os registros do banco de dados. Se a desinfecção for a ação principal a ser executada com o objeto (ou seja, a primeira ação a ser executada com o objeto imediatamente após sua detecção), será criada uma cópia de backup do objeto antes da tentativa de desinfecção. Parte dos dados pode ser perdida durante a desinfecção. Essa cópia de backup poderá ser usada para restaurar o objeto a seu estado original.

DESINFETAR OBJETOS AO REINICIAR

Método de processar objetos infectados que estão sendo usados por outros aplicativos no momento da desinfecção. Consiste em criar uma cópia do objeto infectado, desinfetando a cópia criada e substituindo o objeto original infectado pela cópia após a próxima reinicialização do sistema.

E

EXCLUINDO UM OBJETO

Método de processamento de objetos que os exclui fisicamente de seu local original (disco rígido, pasta, recurso de rede). É recomendável aplicar esse método a objetos perigosos que, por algum motivo, não podem ser desinfetados.

EXCLUSÃO

Exclusão é um objeto excluído da verificação pelo aplicativo da Kaspersky Lab. Você pode excluir arquivos de determinados formatos da verificação , usar uma máscara de arquivos ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objetos, de acordo com a classificação de tipos de ameaça da Enciclopédia de vírus. Cada tarefa pode ser atribuída um conjunto de exclusões.

EXCLUSÃO DE MENSAGENS

Método de processar um email que contém sinais de spam, em que a mensagem é removida fisicamente. É aconselhável aplicar este método a mensagens que contêm spam sem ambigüidade. Antes de excluir a mensagem, uma cópia dele é salva no backup (a menos que a opção tenha sido desativada).

I

IGNORAR OBJETOS

Método de processamento em que um objeto é transmitido ao usuário sem alterações. Se o registro de eventos está ativado para esse tipo de evento, as informações sobre o objeto detectado serão registradas no relatório.

INTERCEPTOR

Subcomponente do aplicativo responsável por verificar tipos específicos de email. O conjunto de interceptores específicos para a sua instalação depende de qual função ou para qual combinação de funções o aplicativo está sendo instalado.

L

LICENÇA ADICIONAL

Uma licença que foi adicionada para a operação do aplicativo da Kaspersky Lab, mas que ainda não foi ativada. A licença adicional entra em vigor quando a licença ativa expira.

LICENÇA ATIVA

A licença usada no momento para a operação de um aplicativo da Kaspersky Lab. A licença define a data de expiração da funcionalidade completa e a diretiva de licenças do aplicativo. O aplicativo não pode ter mais de uma licença com o status ativo.

LIMITE DE ATIVIDADE DE VÍRUS

O nível máximo permissível de um tipo específico de evento em um período limitado que, quando excedido, será considerado como atividade excessiva de vírus e uma ameaça de surto de vírus. Este recursos é significativo durante surtos de vírus e permite ao administrador reagir em tempo hábil a ameaças de surtos de vírus.

LISTA NEGRA DE ARQUIVOS DE CHAVE

Um banco de dados que contêm informações sobre arquivos de chave da Kaspersky Lab cujos proprietários violaram os termos do contrato de licença e informações sobre arquivos de chave emitidos, mas que por algum motivo não foram vendidos ou foram substituídos. Uma lista negra é necessária para a operação dos aplicativos da Kaspersky Lab. O conteúdo do arquivo é atualizado junto com os bancos de dados.

M

MOVENDO OBJETOS PARA A QUARENTENA

Método de processar um objeto potencialmente infetado bloqueando o acesso ao arquivo e movendo-o para o seu local original na pasta Quarentena, onde o objeto é salvo em formato criptografados, o que elimina a ameaça de infecção. Objetos em quarentena podem ser verificados usando bancos de dados de Anti-Virus, analisados pelo administrador, ou enviados ao Kaspersky Lab.

MÁSCARA DE ARQUIVO

Representação de nome de arquivo e extensão usando curingas. Os dois curingas padrão usados em máscaras de arquivos são * e ?, onde * representa qualquer número de caracteres e ? representa qualquer caractere. Com esses curingas, você pode representar qualquer arquivo. Note que o nome e a extensão são sempre separados por um ponto final.

MÁSCARA SUB-REDE

Máscara sub-rede (também conhecida como máscara de rede) e endereço de rede determinam os endereços de computadores em uma rede.

N

NÍVEL DE GRAVIDADE DE EVENTO

Descrição do evento, registrado durante a operação do aplicativo Kaspersky Lab. Há quatro níveis de gravidade:

- **Evento crítico.**
- **Falha funcional.**
- **Advertência.**
- **Mensagem informativa.**

Eventos do mesmo tipo com níveis diferentes de segurança, dependendo da situação em que o evento ocorreu.

NÍVEL RECOMENDADO

Nível de segurança baseado em configurações de aplicativos recomendadas pelos peritos da Kaspersky Lab para oferecer nível otimizado de proteção para o computador. Este nível é configurado para ser usado por padrão.

O

OBJETO OLE

Um objeto anexado ou incorporado a outro arquivo. O aplicativo da Kaspersky Lab permite a verificação de vírus em objetos OLE. Por exemplo, se você inserir uma tabela do Microsoft Office Excel em um documento do Microsoft Office Word, a tabela será verificada como um objeto OLE.

OBJETO INFECTADO

Objeto que contém um código malicioso: ele é detectado quando uma seção do código do objeto corresponde integralmente a uma seção do código de uma ameaça conhecida. A Kaspersky Lab não recomenda usar esses objetos, pois eles podem propiciar a infecção do seu computador.

OBJETO MONITORADO

Um arquivo transferido via protocolos HTTP, FTP, ou SMTP no firewall e enviados ao aplicativo da Kaspersky Lab application para verificação.

OBJETO PERIGOSO

Objeto com vírus. É recomendável não acessar esses objetos, pois isso poderia causar a infecção do seu computador. Quando um objeto infectado é detectado, é recomendável desinfetá-lo usando um dos aplicativos da Kaspersky Lab ou, caso a desinfecção não seja possível, excluí-lo.

OBJETO POTENCIALMENTE INFECTADO

Um objeto que contém o código de um vírus conhecido modificado ou um código que parece com o código de um vírus, mas que ainda não é conhecido pela Kaspersky Lab. Arquivos potencialmente infectados são detectados usando um analisador heurístico.

OBJETO POTENCIALMENTE INFETÁVEL

Um objeto que, devido à sua estrutura ou ao seu formato, pode ser usado por invasores como um "contêiner" para armazenar e distribuir um objeto malicioso. Normalmente, são arquivos executáveis, por exemplo, arquivos com as extensões .com, .exe, .dll, etc. O risco de ativar códigos maliciosos nesses arquivos é bastante alto.

OBJETO SIMPLES

Corpo do email ou anexos simples, por exemplo, um arquivo executável. Consulte também objetos de contêiner.

OBJETO SUSPEITO

Um objeto que contém o código de um vírus conhecido modificado ou um código que parece com o código de um vírus, mas que ainda não é conhecido pela Kaspersky Lab. Objetos suspeitos são detectados usando o analisador heurístico.

OBJETOS DE INICIALIZAÇÃO.

O conjunto de programas necessários para iniciar e operar corretamente o sistema operacional e o software instalado no seu computador. Esses objetos são executados a cada vez que o sistema operacional é inicializado. Há vírus capazes de infectar tais objetos de forma específica, que podem levar, por exemplo, a bloquear o acesso ao sistema operacional.

P

PACOTE DE ATUALIZAÇÃO

Pacote de arquivos para a atualização do software. Ele é baixado da Internet e instalado no computador.

PASTA DE DADOS

A pasta que contém as pastas de serviço e bancos de dados necessários para trabalhar com o aplicativo. Se a pasta de dados é movida, todas as informações que inclui devem ser salvas em outro local.

PRAZO DE VALIDADE DA LICENÇA

Período durante o qual você pode usar todos os recursos do seu aplicativo da Kaspersky Lab. O prazo de validade da licença geralmente é de um ano civil da data da instalação. Depois que a licença expira, o aplicativo terá funcionalidade reduzida. Você não poderá atualizar os bancos de dados do aplicativo.

PROCESSO CONFIÁVEL

O processo do aplicativo cujas operações de arquivos não são monitoradas pelo aplicativo da Kaspersky Lab no modo de proteção em tempo real. Em outras palavras, nenhum objeto executado, aberto, ou salvo pelo processo confiável será verificado.

PROTEÇÃO EM TEMPO REAL

O modo de operação do aplicativo sob o qual os objetos são verificados quanto à presença de código malicioso em tempo real.

O aplicativo intercepta todas as tentativas de abrir qualquer objeto (ler, escrever ou executar) e verifica o objeto quanto a ameaças. Objetos não-infectados são transmitidos ao usuário; objetos que contêm ameaças ou suspeita de ameaças são processados de acordo com as configurações de tarefas (são desinfetados, excluídos ou colocados em quarentena).

PROTEÇÃO MÁXIMA

Nível de segurança para o seu computador correspondente à proteção mais completa que o aplicativo pode oferecer. Neste nível de proteção, todos os arquivos do computador, meios de armazenamento removíveis e unidades de rede são verificadas quanto a vírus se conectadas ao computador.

Q

QUARENTENA

Uma pasta específica na qual são colocados todos os objetos possivelmente infectados detectados durante as verificações ou pela proteção em tempo real.

R

RESTAURAÇÃO

Movendo um objeto original da Quarentena ou Backup para a pasta onde ele foi originalmente encontrado antes de ter sido movido para a Quarentena, desinfetado, ou excluído, ou para uma pasta diferente especificada pelo usuário.

S

SERVIDORES DE ATUALIZAÇÃO DA KASPERSKY LAB

Lista de servidores HTTP e FTP da Kaspersky Lab dos quais o aplicativo baixa atualizações de bancos de dados e módulos para o computador.

SETOR DE INICIALIZAÇÃO DE DISCO

Um setor de inicialização é uma área particular no disco rígido de um computador, ou outro dispositivo de armazenamento de dados. Ele contém informações sobre o sistema de arquivos do disco e um programa de carregamento de inicialização, responsável por iniciar o sistema operacional.

Há vários vírus que infetam os setores de inicialização, que são chamados de vírus de inicialização. O aplicativo da Kaspersky Lab permite verificar os setores de inicialização quanto a vírus e desinfetá-los se uma infecção for encontrada.

STATUS DA PROTEÇÃO

O atual status de proteção, resumindo o grau de segurança do computador.

SURTO DE VÍRUS

Uma série de tentativas de infectar um computador com um vírus.

T

TECNOLOGIA ICHECKER

O iChecker é uma tecnologia que aumenta a velocidade das verificações antivírus por meio da exclusão de objetos que permaneceram inalterados desde a última verificação, desde que os parâmetros de verificação (as configurações e o banco de dados de antivírus) não tenham mudado. As informações de cada arquivo são armazenadas em um banco de dados especial. Essa tecnologia é usada nos modos de proteção em tempo real e de verificação por demanda.

Por exemplo, você tem um arquivo que foi verificado pelo aplicativo da Kaspersky Lab e ao qual foi atribuído o status não infectado. Na próxima verificação, o aplicativo vai ignorar esse arquivo comprimido, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Se você alterou o conteúdo do arquivo comprimido, adicionando um novo objeto a ele, modificou as configurações de verificação ou atualizou o banco de dados de antivírus, o arquivo comprimido será verificado novamente.

Limitações da tecnologia iChecker:

- essa tecnologia não trabalha com arquivos grandes, pois é mais rápido verificar o arquivo que analisar se ele foi modificado desde sua última verificação;
- a tecnologia dá suporte a um número limitado de formatos **(.exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).**

V

VERIFICAÇÃO DE ARMAZENAMENTO

Verificar emails armazenados no servidor de email e o conteúdo de pastas compartilhadas usando a última versão do banco de dados. A verificação é executada em segundo plano e pode rodar usando uma programação sob demanda.

Todo o armazenamento de pastas e caixa de entrada são verificados. Nenhum vírus pode ser detectado durante a verificação sobre o que não há informação no banco de dados em verificações anteriores.

VERIFICAÇÃO SOB DEMANDA

Modo operacional do aplicativo da Kaspersky Lab iniciado pelo usuário e que pode ter como alvo quaisquer mensagens no computador.

VÍRUS DE INICIALIZAÇÃO

Um vírus que infecta os setores de inicialização do disco rígido de um computador. O vírus força o sistema a baixá-lo na memória durante a reinicialização e dirigir o controle do código do vírus em vez do código original de carregamento de inicialização.

VÍRUS DESCONHECIDO

Um novo vírus sobre o qual não há informações nos bancos de dados. Geralmente, vírus desconhecidos são detectados pelo aplicativo em objetos que usam analisadores heurísticos, e esses objetos são classificados como potencialmente infectados.

KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997. Hoje é o desenvolvedor russo líder de uma ampla gama de produtos de software de segurança da informação de alto desempenho, incluindo sistemas antivírus, Antispam e anti-hacking.

A Kaspersky Lab é uma empresa internacional. Com sede na Federação Russa, a empresa possui escritórios no Reino Unido, França, Alemanha, Japão, países da Benelux, China, Polônia, Romênia e USA (Califórnia). Um novo escritório da empresa, o Centro de Pesquisas Antivírus Europeia, foi recentemente inaugurado na França. A rede de parceiros da Kaspersky Lab possui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de mil especialistas altamente qualificados, incluindo 10 detentores de MBA e 16 PhD. Todos os especialistas antivírus seniores da Kaspersky Lab são membros da Computer Anti-Virus Researchers Organization (CARO).

Os ativos mais valiosos de nossa empresa são o conhecimento exclusivo e a habilidade coletiva acumulados durante os catorze anos de luta contínua contra os vírus de computador. As análises criteriosas das atividades de vírus de computador capacitam os especialistas da empresa a antecipar as tendências no desenvolvimento de malware e fornecer aos nossos usuários proteção oportuna contra novos tipos de ataques. Essa vantagem é a base dos produtos e serviços da Kaspersky Lab. Os produtos da empresa permanecem um passo à frente de outros vendedores no fornecimento de cobertura antivírus abrangente aos nossos clientes.

Anos de trabalho árduo tornaram a empresa um dos principais desenvolvedores de software antivírus. A Kaspersky Lab foi a primeira a desenvolver muitos dos padrões modernos de software antivírus. O produto mais importante da empresa, o Kaspersky Anti-Virus®, protege confiavelmente todos os tipos de sistemas de computador contra ataques de vírus, incluindo estações de trabalho, servidores de arquivo, sistemas de correio, firewalls, gateways da Internet e computadores portáteis. Suas ferramentas de gerenciamento fáceis de usar maximizam a automação da proteção antivírus de computadores e rede corporativas. Um grande número de desenvolvedores no mundo inteiro usa o núcleo do Kaspersky antivírus em seus produtos, incluindo a Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab dispõem de vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a conformidade total com seus requisitos empresariais específicos. Projetamos, implementamos e damos suporte aos sistemas antivírus corporativos. O banco de dados antivírus da Kaspersky Lab é atualizado por hora. A empresa fornece aos seus clientes serviço de Suporte Técnico 24 horas em vários idiomas.

Caso tenha perguntas, comentários ou sugestões, você pode nos contatar através de nossos distribuidores, ou a Kaspersky Lab diretamente. Ficaremos contentes em assisti-lo, pelo telefone ou email, em qualquer assunto relacionado aos nossos produtos. Você receberá respostas completas e abrangentes para todas as suas perguntas.

Site oficial da Kaspersky Lab:	http://brazil.kaspersky.com/
Enciclopédia de vírus:	http://www.viruslist.com
Laboratório de antivírus:	newvirus@kaspersky.com (somente para envio de arquivos comprimidos de objetos suspeitos) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (para consultas com analistas de vírus)

CONTRATO DE LICENÇA

IMPORTANTE ADVERTÊNCIA LEGAL PARA TODOS OS USUÁRIOS: LEIAM COM CUIDADO O SEGUINTE CONTRATO LEGAL ANTES DE COMEÇAR A USAR O APLICATIVO.

CLICANDO NO BOTÃO "ACEITO" NA JANELA DE CONTRATO DE LICENÇA OU AO DIGITAR O(S) SÍMBOLO(S) CORRESPONDENTE(S) VOCÊ ESTARÁ CONCORDANDO EM VINCULAR-SE PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESTA AÇÃO SIMBOLIZA A SUA ASSINATURA E A SUA CONCORDÂNCIA EM VINCULAR-SE PELOS TERMOS DO PRESENTE CONTRATO, TORNANDO-SE PARTE DELE E CONCORDANDO SER ESTE CONTRATO EXECUTÁVEL COMO QUALQUER OUTRO CONTRATO NEGOCIADO E ASSINADO POR VOCÊ**. CASO VOCÊ NÃO CONCORDE COM TODOS OS TERMOS E CONDIÇÕES DO PRESENTE CONTRATO, CANCELE A INSTALAÇÃO DO APLICATIVO E NÃO O INSTALE.

APÓS CLICAR NO BOTÃO ACEITO NA JANELA DE CONTRATO DE LICENÇA OU AO DIGITAR O(S) SÍMBOLO(S) CORRESPONDENTE(S), VOCÊ TERÁ O DIREITO DE USAR O APLICATIVO EM CONFORMIDADE COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. **Definições**

1.1. **Aplicativo** significa o aplicativo incluindo quaisquer atualizações e materiais relacionados.

1.2. **Titular** (proprietário de todos os direitos, quer sejam exclusivos ou não ao Aplicativo) significa a Kaspersky Lab ZAO, uma empresa constituída nos termos da legislação da Federação Russa.

1.3. **Computador(es)** significa(am) equipamento(s), incluindo computadores pessoais, computadores portáteis, estações de trabalho, assistentes digitais pessoais, 'telefones inteligentes', aparelhos de mão ou outros dispositivos eletrônicos para os quais o Aplicativo foi projetado, onde o Aplicativo será instalado e/ou usado.

1.4. **Usuário Final (Você / Seu)** significa instalação(ões) individual(ais) ou usar o Aplicativo em seu próprio nome ou de quem esteja legalmente usando uma cópia do Aplicativo; ou, se o Aplicativo está sendo baixado ou instalado em nome de uma organização, tal como um empregador, *"Você"* significa ainda a organização para a qual o Aplicativo é baixado ou instalado, declarando-se, para fins do presente instrumento, que tal organização tenha autorizado a pessoa aderindo a este contrato a fazê-lo em seu nome. Para os efeitos do presente documento o termo *"organização"*, inclui, entre outros, qualquer parceria, sociedade de responsabilidade limitada, corporação, associação, sociedade de capital aberto, fundo fiduciário, empreendimento conjunto, organização do trabalho, organização sem personalidade jurídica ou autoridade governamental.

1.5. **Parceiro(s)** significa organização(ões) ou indivíduo(s) que distribui(em) o Aplicativo, tendo como base um contrato e licenciamento com o Titular.

1.6. **Atualização(ões)** significa(am) todas as atualizações, revisões, correções, aprimoramentos, emendas, modificações, cópias, adições ou pacotes de manutenção etc.

1.7. **Manual do usuário** significa manual do usuário, guia do administrador, livro de referência e explicações correlatas ou outros materiais.

2. **Licenciamento**

2.1. O Titular concede a Você, por este instrumento, uma licença não exclusiva para armazenar, carregar, instalar, executar e exibir ("usar") o Aplicativo em um determinado número de computadores, a fim de ajudar a proteger o seu computador, no qual o Aplicativo é instalado, das ameaças descritas no Manual do usuário, de acordo com todos os requisitos técnicos descritos no Manual do usuário e de acordo com os termos e condições do presente Contrato (a "Licença"), sendo tal Licença aceita por você:

Versão de avaliação. Se tiver recebido, baixado e/ou instalado uma versão de avaliação do Aplicativo e lhe é concedida nesse ato uma licença de avaliação do Aplicativo, você pode usar o Aplicativo apenas para fins de avaliação e apenas durante o único período de avaliação aplicável, salvo indicação contrária, a partir da data da instalação inicial. Qualquer uso do Aplicativo para outros fins ou para além do período de avaliação aplicável é estritamente proibido.

Aplicativo para múltiplos ambientes; Aplicativo para múltiplos idiomas; Aplicativo para mídia dupla; cópias múltiplas; pacotes. Caso você use diferentes versões do Aplicativo ou edições em diferentes idiomas do Aplicativo, caso receba o Aplicativo em múltiplos meios de comunicação, caso receba várias cópias do Aplicativo ou caso tenha recebido o Aplicativo em conjunto com outro aplicativo, o número total permitido dos seus computadores nos quais todas as versões do Aplicativo são instaladas deve corresponder ao número de licenças que tenha obtido a partir do Titular, uma vez que, *salvo* se os termos e condições de licenciamento disponham de outra forma, cada licença adquirida lhe dá o direito de instalar e usar o aplicativo em tal número de Computador(es), conforme especificado nas Cláusulas 2.2 e 2.3.

2.2. Caso o Aplicativo tenha sido adquirido por meio físico, Você tem o direito de usar o Aplicativo para a proteção de tal número de Computador(es), conforme especificado no pacote do Aplicativo.

2.3. Caso o Aplicativo tenha sido adquirido na Internet, Você tem o direito de usar o Aplicativo para a proteção de tal número de computadores que foi especificado quando Você comprou a licença para o Aplicativo.

2.4. Você tem o direito de fazer uma cópia do Aplicativo apenas para fins de cópia de segurança, e apenas para substituir a cópia legalmente de sua propriedade, caso essa cópia seja extraviada, destruída ou se tornar inutilizável. Tal cópia de segurança não pode ser utilizada para outros fins, devendo ser destruída quando você perder o direito ao uso do Aplicativo ou quando a Sua licença vencer ou for rescindida, por qualquer outro motivo, de acordo com a legislação em vigor no país da sua residência principal ou no país onde Você está usando o Aplicativo.

2.5. Você pode transferir a licença não exclusiva para usar o Aplicativo para outras pessoas físicas ou jurídicas no âmbito da licença concedida pelo Titular a Você, desde que o beneficiário concorde em ficar vinculado por todos os termos e condições deste Contrato e substituí-lo na íntegra na licença concedida pelo Titular. Caso Você transfira integralmente os direitos concedidos pelo Titular para o uso do Aplicativo, Você deve destruir todas as cópias do Aplicativo, incluindo a cópia de segurança. Caso Você seja beneficiário de uma transferência de licença, deverá concordar em obedecer todos os termos e condições deste Contrato. Caso Você não concorde em vincular-se por todos os termos e condições deste Contrato, você não pode instalar e/ou usar o Aplicativo. Você também concorda, na qualidade de beneficiário de uma licença transferida, que Você não tem direitos adicionais ou melhores do que os do usuário final original que adquiriu o aplicativo do Titular.

2.6. A partir do período de ativação do Aplicativo ou após a instalação da licença (com exceção de uma versão de avaliação do Aplicativo) Você tem o direito de receber os seguintes serviços para o período definido especificado no pacote do Aplicativo (caso o Aplicativo tenha sido adquirido em meio físico) ou especificado durante a aquisição (caso o Aplicativo tenha sido adquirido na Internet):

- Atualizações do aplicativo na Internet, quando e como o Titular as publicar em sua página, ou por meio de outros serviços em linha. Quaisquer atualizações que você venha a receber tornam-se parte do Aplicativo, aplicando-se às mesmas os termos e condições do presente Contrato;
- Assistência técnica na Internet e assistência técnica por linha telefônica direta.

3. **Ativação e prazo**

3.1. Caso você modifique o seu computador ou faça alterações em aplicativos de outros fornecedores nele instalados, o Titular poderá solicitar que Você repita a ativação do Aplicativo ou instalação da licença. O Titular reserva-se o direito de usar todos os meios e procedimentos de verificação para verificar a validade da Licença e/ou legalidade de cópias do Aplicativo instaladas e/ou usadas em seu computador.

3.2. Caso o Aplicativo tenha sido adquirido em meio físico, o Aplicativo poderá ser usado, mediante aceitação do presente Contrato, durante o período especificado na embalagem, o qual inicia-se após a aceitação do presente Contrato.

3.3. Caso o Aplicativo tenha sido adquirido na Internet, o Aplicativo poderá ser usado, mediante aceitação do presente Contrato, durante o período especificado durante a compra.

3.4. Você tem o direito de usar uma versão do Aplicativo, conforme disposto na Cláusula 2.1, sem qualquer encargo, pelo período único de avaliação (30 dias) aplicável a partir do momento de ativação do Aplicativo, de acordo com o presente Contrato, *desde que* a versão de avaliação não lhe conceda nenhum direito a Atualizações e assistência técnica na Internet nem a assistência técnica por linha telefônica direta.

3.5. Sua licença de uso do Aplicativo é restrita ao período de tempo especificado nas Cláusulas 3.2 ou 3.3 (conforme aplicável), e o período restante pode ser visualizado pelo meio descrito no Manual do usuário.

3.6. Se você tiver comprado o Aplicativo com o objetivo do mesmo ser usado em mais de um Computador, a sua Licença de uso do Aplicativo estará limitada ao período de tempo contado a partir da data de ativação do Aplicativo ou da instalação da licença no primeiro computador.

3.7. Sem prejuízo para quaisquer outras soluções legais ou pelo princípio da equivalência que o Titular possa vir a ter, em caso de qualquer violação de quaisquer termos e condições deste Contrato por Sua parte, o Titular terá, a qualquer momento, sem aviso prévio ao usuário, o direito de rescindir esta Licença para o uso do Aplicativo, sem reembolso do preço de compra ou qualquer parte dele.

3.8. Você concorda que, ao usar o Aplicativo e ao usar qualquer relatório ou informação obtida como resultado da utilização deste Aplicativo, você irá cumprir todas as leis e regulamentos internacionais, nacionais, estaduais, regionais e locais, incluindo, entre outras, as leis de privacidade, do direito autoral, do controle de exportação e a lei sobre obscenidade.

3.9. Salvo se expressamente disposto aqui, você não poderá transferir ou atribuir nenhum dos direitos concedidos ao abrigo deste Contrato ou qualquer uma das suas obrigações relativas ao presente instrumento.

4. **Assistência técnica**

A assistência técnica descrita na Cláusula 2.6 do presente Contrato será fornecida a Você quando a mais recente atualização do Aplicativo for instalada (com exceção de uma versão de avaliação do Aplicativo).

Serviço de suporte técnico: http://support.kaspersky.com

5. **Limitações**

5.1. Você não deve simular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou fazer engenharia reversa no Aplicativo, nem desmontar ou criar trabalhos derivados do Aplicativo ou de qualquer parte dele, com a única exceção de um direito não renunciável concedido a Você pela legislação aplicável, e você não deve reduzir de nenhuma maneira qualquer parte do Aplicativo para o formato humano legível ou transferir o Aplicativo licenciado ou qualquer subconjunto do Aplicativo licenciado, nem permitir que terceiros o façam, exceto nos casos em que a restrição anterior seja expressamente proibida pela lei aplicável. Nem o código binário do Aplicativo nem o código-fonte pode ser usado ou submetido a engenharia reversa para recriar o algoritmo do programa, que é exclusivo do Titular. Todos os direitos não expressamente concedidos neste Contrato são reservados pelo Titular e/ou seus fornecedores, conforme aplicável. Qualquer uso não autorizado do Aplicativo resultará na rescisão imediata e automática do presente Contrato e da Licença aqui concedida, podendo resultar em processo penal e/ou cível contra Você.

5.2. Você não deve transferir os direitos de uso do Aplicativo a terceiros, salvo conforme estabelecido na Cláusula 2.5 do presente Contrato.

5.3. Você não deve fornecer o código de ativação e/ou o arquivo da chave de licença a terceiros, nem permitir que terceiros tenham acesso ao código de ativação e/ou a chave de licença, os quais são considerados dados confidenciais do Titular, e você tomará todas as precauções, dentro do razoável, para proteger o código de ativação e/ou a chave de licença, de boa-fé, já que você pode transferir o código de ativação e/ou a chave de licença a terceiros, conforme estipulado na Cláusula 2.5 do presente Contrato.

5.4. Você não pode alugar, arrendar ou emprestar o Aplicativo a terceiros.

5.5. Você não deve usar o Aplicativo para a criação de dados ou aplicativos usados para detecção, bloqueio ou tratamento das ameaças descritas no Manual do usuário.

5.6. O Titular tem o direito de bloquear o arquivo da chave ou rescindir a Sua Licença para uso do Aplicativo caso Você viole qualquer dos termos e condições deste Contrato, sem qualquer restituição a Você.

5.7. Caso Você esteja usando a versão de avaliação do Aplicativo, não terá o direito de receber a assistência técnica especificada na Cláusula 4 do presente Contrato, nem terá o direito de transferir a licença ou os direitos de uso do Aplicativo para qualquer terceiro.

6. **Garantia restrita e exclusão**

6.1. O Titular garante que o Aplicativo irá desempenhar substancialmente, de acordo com as especificações e descrições estabelecidas no Manual do usuário, *desde que, entretanto*, a referida garantia restrita não se aplique ao seguinte: (w) deficiências de seu computador e violação relacionada para as quais o Titular renuncia expressamente a qualquer responsabilidade da garantia; (x) avarias, defeitos ou falhas resultantes de uso

indevido, abuso, acidente, negligência, instalação, operação ou manutenção imprópria; furto; vandalismo; atos fortuitos; atos de terrorismo; falhas ou picos de energia; acidente, alteração, modificações ou reparos não permitidos por qualquer terceiro que não seja o Titular, ou quaisquer outros terceiros ou Suas ações ou causas além do controle razoável pelo Titular; (y) qualquer defeito, não divulgado por Você ao Titular o mais rapidamente possível, após o defeito aparecer pela primeira vez; e (z) causados por incompatibilidade de componentes de equipamento e/ou aplicativo instalado em Seu computador.

6.2. Você reconhece, aceita e concorda que nenhum aplicativo está isento de erros, sendo aconselhado a realização de cópia de segurança no computador, com uma frequência e confiabilidade adequadas para Você.

6.3. O Titular não oferece qualquer garantia de que o Aplicativo irá funcionar corretamente em caso de violação dos termos e condições descritos no Manual do usuário ou no presente Contrato.

6.4. O Titular não garante que o Aplicativo irá funcionar corretamente se Você não baixar regularmente as Atualizações especificadas na Cláusula 2.6 do presente Contrato.

6.5. O Titular não garante proteção contra as ameaças descritas no Manual do usuário após o vencimento do prazo especificado nas Cláusulas 3.2 ou 3.3 do presente Contrato ou após a rescisão, por qualquer motivo, da Licença de uso do Aplicativo.

6.6. O APLICATIVO É FORNECIDO "TAL COMO SE ENCONTRA", E O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA QUANTO A SEU USO OU DESEMPENHO. SALVO POR QUALQUER GARANTIA, CONDIÇÃO, DECLARAÇÃO OU TERMO, NA MEDIDA EM QUE NÃO PODE SER EXCLUÍDA OU RESTRITA PELA LEGISLAÇÃO APLICÁVEL, O TITULAR E SEUS PARCEIROS NÃO DÃO NENHUMA GARANTIA, CONDIÇÃO, DECLARAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, USO OU DE ALGUMA OUTRA MANEIRA) QUANTO A QUALQUER ASSUNTO, INCLUINDO, ENTRE OUTROS, A NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS, COMERCIABILIDADE, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE PARA DETERMINADO PROPÓSITO. VOCÊ ASSUME TODAS AS FALHAS E TODO O RISCO QUANTO AO DESEMPENHO E RESPONSABILIDADE DE SELEÇÃO DO APLICATIVO PARA ALCANÇAR SEUS RESULTADOS PRETENDIDOS, BEM COMO PARA A INSTALAÇÃO, USO E RESULTADOS OBTIDOS PELO APLICATIVO. SEM PREJUÍZO DAS DISPOSIÇÕES ANTERIORES, O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA QUE O APLICATIVO ESTARÁ LIVRE DE ERROS, INTERRUPÇÕES OU OUTRAS FALHAS, NEM QUE O APLICATIVO ATENDERÁ QUALQUER OU TODOS OS SEUS REQUISITOS, QUER OU NÃO DIVULGADOS AO TITULAR.

7. **<u>Exclusão e limitação da responsabilidade</u>**

NA MEDIDA DO PERMITIDO PELA LEGISLAÇÃO APLICÁVEL, EM NENHUM CASO O TITULAR OU SEUS PARCEIROS SERÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, INCIDENTAIS, PUNITIVOS, INDIRETOS, CONSEQUÊNCIAIS OU QUAISQUER DANOS (INCLUINDO, ENTRE OUTROS, DANOS POR PERDA DE RECEITA OU CONFIDENCIAIS OU OUTRAS INFORMAÇÕES, POR INTERRUPÇÃO DOS NEGÓCIOS, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANO E PERDA DE DADOS OU PROGRAMAS, POR NÃO CUMPRIMENTO DE QUALQUER DEVER INCLUINDO QUALQUER OBRIGAÇÃO LEGAL, DIREITO DE BOA-FÉ OU DIREITO DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PREJUÍZOS ECONÔMICOS, E QUAISQUER OUTRAS PERDAS PECUNIÁRIAS OU OUTRA PERDA) DECORRENTES DE OU DE ALGUMA MANEIRA RELACIONADOS AO USO OU À IMPOSSIBILIDADE DE USAR O APLICATIVO, A PROVISÃO OU FALTA DE PRESTAÇÃO DE APOIO OU OUTROS SERVIÇOS, INFORMAÇÕES, APLICATIVO E CONTEÚDO RELACIONADO POR MEIO DO APLICATIVO OU DE OUTROS DECORRENTES DO USO DO APLICATIVO OU DE QUALQUER OUTRO RESULTANTE OU RELACIONADO COM QUALQUER DISPOSIÇÃO DO PRESENTE CONTRATO, OU DECORRENTE DE QUALQUER VIOLAÇÃO DE CONTRATO OU QUALQUER OFENSA (INCLUINDO NEGLIGÊNCIA, DETURPAÇÃO, QUALQUER RESPONSABILIDADE OU OBRIGAÇÃO RIGOROSA), OU QUALQUER VIOLAÇÃO DA GARANTIA DE DEVERES ESTATUTÁRIOS OU QUALQUER QUEBRA DA GARANTIA DO TITULAR OU QUALQUER UM DE SEUS PARCEIROS, MESMO SE O TITULAR OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DOS REFERIDOS DANOS.

VOCÊ CONCORDA QUE EM CASO DE O TITULAR E/OU SEUS PARCEIROS SEREM JULGADOS RESPONSÁVEIS, A RESPONSABILIDADE DO TITULAR E/OU DOS SEUS PARCEIROS ESTARÁ RESTRITA AOS CUSTOS DO APLICATIVO. EM NENHUM CASO, A RESPONSABILIDADE DO TITULAR E/OU SEUS PARCEIROS EXCEDERÁ O PREÇO PAGO AO TITULAR OU AO PARCEIRO PELO APLICATIVO (TAL COMO APLICÁVEL).

NADA NESTE CONTRATO EXCLUI OU LIMITA QUALQUER REIVINDICAÇÃO POR MORTE E LESÃO CORPORAL. AINDA NO CASO DE QUALQUER RENÚNCIA, EXCLUSÃO OU RESTRIÇÃO NESTE CONTRATO NÃO PODER SER EXCLUÍDA OU RESTRITA DE ACORDO COM A LEGISLAÇÃO APLICÁVEL, NESSE CASO, APENAS A REFERIDA RENÚNCIA, EXCLUSÃO OU RESTRIÇÃO NÃO IRÁ SE APLICAR A VOCÊ, E VOCÊ CONTINUARÁ VINCULADO POR TODAS AS RENÚNCIAS, EXCLUSÕES E RESTRIÇÕES REMANESCENTES.

8. **GNU e outras licenças de terceiros**

O Aplicativo pode incluir alguns programas de aplicativo que são licenciados (ou sublicenciados) para o usuário sob Licença Pública Geral GNU (GNU General Public License, GPL) ou outras licenças similares de aplicativo livre, que, entre outros direitos, permitem ao usuário copiar, modificar e redistribuir determinados programas, ou partes dos mesmos, bem como ter acesso ao código-fonte ("Aplicativo com Código Aberto"). Caso essas licenças exijam que, para qualquer aplicativo que é distribuído a alguém em formato binário executável, o código-fonte também seja disponibilizado a esses usuários, então ele deve ser disponibilizado por meio do envio de uma solicitação para source@kaspersky.com ou o código fonte fornecido juntamente com o Aplicativo. Se quaisquer licenças de Aplicativo com Código Aberto exigirem que o Titular propicie direitos para usar, copiar ou modificar um programa de Aplicativo com Código Aberto que é mais abrangente que os direitos concedidos no presente Contrato, os referidos direitos devem ter primazia sobre os direitos e restrições no presente instrumento.

9. **Titularidade da propriedade intelectual**

9.1 Você concorda que o Aplicativo e a autoria, sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Aplicativo, são propriedade intelectual e/ou segredos industriais valiosos do Titular ou de seus parceiros, e que o Titular e seus parceiros, conforme o caso, são protegidos pelo direito civil e penal e pela lei de direitos autorais, segredos industriais, marcas e patentes da Federação Russa, da União Europeia e dos EUA, bem como de outros países e tratados internacionais. O presente Contrato não concede a Você nenhum direito à propriedade intelectual, incluindo todas as marcas comerciais ou marcas de serviço do Titular e/ou seus parceiros ("Marcas"). Você poderá usar as marcas comerciais apenas nas saídas impressas produzidas pelo Aplicativo, de acordo com a prática aceita de marcas comerciais, incluindo a identificação do nome do proprietário da marca comercial. Essa utilização de qualquer marca comercial não lhe dá qualquer direito de propriedade na referida marca. O Titular e/ou seus parceiros possuem e detêm todos os direitos, títulos e interesses relativos ao Aplicativo, incluindo, entre outros, quaisquer correções de erros, melhorias, atualizações ou outras modificações ao Aplicativo, sejam realizadas pelo Titular ou por qualquer terceiro, e todos os direitos autorais, patentes, direitos a segredos comerciais, marcas comerciais e outros direitos de propriedade intelectual contidos neste instrumento. A sua posse, instalação ou uso do Aplicativo não transfere para você qualquer título de propriedade intelectual sobre o Aplicativo, e você não poderá adquirir direitos sobre o Aplicativo, salvo conforme expressamente previsto no presente Contrato. Todas as cópias do Aplicativo feitas em virtude deste instrumento devem conter as mesmas advertências sobre a propriedade que aparecem no Aplicativo. Salvo conforme indicado neste documento, este Contrato não lhe concede direitos de propriedade intelectual ao Aplicativo, e Você reconhece que a Licença, conforme definido mais pormenorizadamente a seguir, concedida ao abrigo do presente Contrato, só lhe garante um direito de uso restrito, nos termos e condições do presente Contrato. O Titular reserva todos os direitos não expressamente concedidos a você no presente Contrato.

9.2 Você reconhece que o código-fonte, o código de ativação e/ou o arquivo de chave de licença para o Aplicativo são propriedade do Titular, constituindo segredos industriais do Titular. Você concorda em não modificar, adaptar, traduzir, fazer engenharia reversa, descompilar, desmontar ou tentar, de qualquer outra forma, descobrir o código-fonte do Aplicativo.

9.3 Você concorda em não modificar ou alterar o Aplicativo por qualquer forma. Você não pode remover ou alterar qualquer advertência de direitos autorais ou outras advertências sobre a propriedade de quaisquer cópias do Aplicativo.

10. **Lei aplicável; arbitragem**

Este Contrato será regido e interpretado de acordo com as leis da Federação Russa, sem referência a conflitos de leis e princípios. Este Contrato não será regido pela Convenção das Nações Unidas sobre Contratos para a Venda Internacional de Mercadorias, cuja aplicação está expressamente excluída. Qualquer litígio decorrente da interpretação ou aplicação dos termos e condições deste Contrato ou qualquer violação destes deve, se não for resolvida por negociação direita, ser resolvida no Tribunal de Arbitragem Comercial Internacional da Câmara de Comércio e Indústria da Federação Russa em Moscou, Federação Russa. Qualquer adjudicação proferida pelo árbitro será final e vinculativa para as partes, podendo ainda qualquer julgamento sobre tal decisão arbitral ser executado em qualquer tribunal de jurisdição competente. Nada na presente Seção 10 deverá impedir uma Parte de buscar ou obter reparação justa em tribunal competente, quer antes, durante ou depois dos processos de arbitragem.

11. **Prazo para interposição de ações judiciais**

Nenhuma ação, independentemente da forma, decorrente das transações no âmbito do presente Contrato, pode ser interposta por qualquer uma das partes aqui mencionadas após 1 (um) ano de a ação ter ocorrido, ou foi constatado ter ocorrido, salvo ação por violação dos direitos de propriedade intelectual, a qual pode ser instaurada dentro do máximo prazo legal aplicável.

12. **Totalidade do contrato; divisibilidade; princípio da não renúncia**

Este Contrato é o contrato integral entre você e o Titular, substituindo quaisquer outros contratos, propostas, comunicações ou publicidade anterior, sendo verbais ou escritos, com relação ao Aplicativo ou ao objeto do presente Contrato. Você reconhece que leu este Contrato, compreende o mesmo e concorda em vincular-se por seus termos e condições. Caso qualquer disposição do presente Contrato seja constatada por um tribunal de jurisdição competente como inválida, nula ou inexequível, por qualquer motivo, no todo ou em parte, essa disposição será interpretada de maneira mais restritiva para que se torne legal e aplicável, e o Contrato não irá sucumbir em seu todo por conta da mesma, permanecendo o restante do Contrato em plena vigência e efeito até o limite máximo permitido pela lei ou por similitude, preservando simultaneamente, na medida do possível, a sua intenção original. Nenhuma renúncia de qualquer disposição ou condição aqui contida será válida, a menos que seja feita por escrito e assinada por você e por um representante autorizado do Titular, sendo que nenhuma renúncia de qualquer violação de quaisquer disposições do presente Contrato constituirá renúncia quanto a qualquer violação prévia, concomitante ou posterior. A falha por parte do Titular em insistir ou aplicar o desempenho rigoroso de qualquer disposição do presente Contrato ou de qualquer direito não deve ser interpretada como renúncia de qualquer disposição ou direito.

13. **Informações para contato**

Caso tenha quaisquer perguntas relativas a este Contrato, ou caso deseje entrar em contato com o Titular, por qualquer motivo, favor entrar em contato com o nosso Departamento de Atendimento ao Cliente:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd

Moscou, 123060

Federação Russa

Tel: +7-495-797-8700

Fax: +7-495-645-7939

Correio eletrônico: info@kaspersky.com

Página na Internet: www.kaspersky.com

INDEX

A

B

C

D

E

I

J

K

M

N

Q

R

S

V

Z